CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS DE BLUE TEAM Y RED TEAM

NUBIA PATRICIA CACUA PATIÑO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C.
2022

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS DE BLUE TEAM Y RED TEAM

NUBIA PATRICIA CACUA PATIÑO

Documento Técnico para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Nombre
Luis Fernando Zambrano Hernandez
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C.
2022

TABLA DE CONTENIDO

LISTA DE FIGURAS

RESUMEN

La ciberseguridad ha tomado poder en los últimos años dentro de las empresas grandes o pequeñas, públicas o privadas puesto que todos los sistemas de información pueden ser atacados, dañados, borrados y/o robados, causándole gran daño, teniendo en cuenta que la información que tenemos guardada es el principal activo de toda persona o institución.

Por eso, a lo largo de este trabajo se puede ver que en Colombia hay legislaciones y leyes para protegernos, herramientas y equipos de personas profesionales con capacidades tanto en el campo de ciberseguridad, con conocimiento de las leyes y sobre todo ética personal y profesional para desarrollar el trabajo de la manera más profesional, transparente y responsable posible para enfrentar la ciberdelincuencia.

Palabras clave: Amenaza, ataques, Ciberseguridad, leyes, vulnerabilidad

ASBTRACT

Cibersecurity has become a very important issue within large or small, public or private companies, since all information systems can be attacked, damaged, deleted and/or stolen, causing great damage, considering that the information It is the main asset of any company.

Therefore, throughout this work it can be seen that we have legislation and laws to protect ourselves, tools and teams of professional people with capabilities both in the field of cybersecurity, with knowledge of the laws and above all personal and professional ethics to develop the I work in the most professional, transparent and responsible way possible to deal with cybercrime.

GLOSARIO

Ataque Cibernético: irrupción a los sistemas por parte de delincuentes cibernéticos buscando obtener información o simplemente romper las defensas de los sistemas operativos.

BlueTeam: Equipos de trabajo que mantienen la defensa de las empresas ante posibles ataques cibernéticos.

CVE: Es un listado de nombres de archivos estandarizados donde se han identificado vulnerabilidades y por el cual podemos conocer el nivel de magnitud de las fallas o errores dentro del sistema**.**

Incidente: Eventos ocurrentes que afectan los sistemas en la confidencialidad, disponibilidad e integridad de la información de las empresas y que pueden llegar a causar mucho daño dentro de ellas.

RedTeam: Equipos de trabajo que realizan ataques a las empresas bajo ambientes controlados para conocer sus vulnerabilidades y fallas.

Vulnerabilidad: Falla o error que puede estar presente en los sistemas que comprometen la seguridad de la empresa y de los cuales los ciberdelincuentes se pueden aprovechar para realizar ataques**.**

INTRODUCCIÓN

Con este trabajo se pretende consultar las normas y leyes que han regido desde los años ochenta (80) en Colombia, observando jurídicamente como avanzamos en temas de protección de datos personales. Además, de analizar las etapas del pentesting, el cual es uno de los métodos más utilizados por los equipos de seguridad informática en las empresas ya sean grande o pequeñas; este tipo de pruebas pueden dar una mayor visión de las brechas de seguridad, fallos o debilidades que tienen las mismas y como atacarlas para mejorar la seguridad.

Además de realizar la verificación de los acuerdos de confidencialidad de HACKERS SECURITY y realizar un análisis legal del mismo revisando que se cumpla con las leyes establecidas y que no haya situaciones ilícitas y si es el caso evidenciando hechos de corrupción dentro de los contratos de las empresas.

Por otro lado, vamos a conocer un poco más de la operación Andrómeda donde veremos que la información es poder. El que tenga el conocimiento del manejo de la información tiene el poder para hacer crecer o para destruir, vamos a conocer un poco sobre el caso de la OPERACIÓN ANDROMEDA BUGGLY.

También, crear un ambiente controlado de pruebas para realizar el proceso de investigación de las vulnerabilidades, ataques y fallas y fuga de información que se han presentado en los equipos de cómputo de la empresa, esto se realiza buscando las mínimas alteraciones en el trabajo de la empresa.

Por último, se indagará sobre lo que se debería hacer en ataques en tiempo real, además, conocer las características principales de lo que es un SIEM y definir herramientas de contención de ataques informáticos

1. OBJETIVOS

1.1 Objetivo General

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

1.2 Objetivos Específicos

- Evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales para adquirir el conocimiento necesario y ponerlo en práctica con casos de la vida real.

- Identificar posibles vulneraciones a la ley 1273 para prevenir posibles abusos y delitos informáticos que quieran hacer pasar por legales y tomar las medidas necesarias ante las entidades correspondientes.

- Indagar sobre lo que se haría si llegara a encontrarse un ataque en tiempo real, para evitar la vulneración a los sistemas de información como robo, daño, secuestro o eliminación de datos en un ciberataque en real.

2. ETAPA 1 - CONCEPTOS EQUIPOS DE SEGURIDAD

2.1 Legislación y Leyes

En la legislación colombiana desde los años 1980 se ha dado iniciativa a generar leyes que propendan por el bien informático de los colombianos.

Las siguientes son las leyes o decretos generados desde entonces:

Ley 100 de 1980: “Por la Cual se expide el nuevo código penal”.[1]

Ley 23 de 1982: “trata de derechos de Autor”, esta ley está vigente, no obstante, ha sufrido cambios.[2]

Desde el año de 1990 se generaron varias leyes asociadas a la preservación de la información digital:

La Constitución Política de Colombia de 1991.En el Titulo II, "De los derechos, las garantías y los deberes", Cap. I. "De los Derechos Fundamentales", Art. 15, "Derecho a la intimidad personal y familiar", constitucionaliza los derechos a la intimidad y el habeas data, al fusionarlos en un mismo artículo, bajo la fórmula siguiente: "Todas las personas tienen derecho a su intimidad...Del mismo modo, tiene derecho a conocer, actualizar y rectificar las informaciones..." entendiendo el

[1] DELITOS INFORMATICOS. [Consulta: 31 de agosto del 2022]. [Página Web]. Disponible en: https://1library.co/document/q76wroky-delitos-informaticos-y-marco-normativo-en-colombia.html

[2] DELITOS INFORMATICOS. [Consulta: 31 de agosto del 2022]. [Página Web]. Disponible en: https://1library.co/document/q76wroky-delitos-informaticos-y-marco-normativo-en-colombia.html

constituyente del 91, que éste último es una consecuencia lógica de la estructuración de la intimidad y no otro derecho también fundamental que tiene su sustento en el derecho a la información (Art. 20 y 73 ibidem), en el desarrollo de la personalidad (Art. 16 id.) y en los valores constitucionales de la dignidad, respeto y solidaridad humanos (Art. 1 id.) que no sólo a la intimidad puede servir de sustento, afección, restricción o límite o auto límite constitucional sino al cúmulo de derechos fundamentales previstos en el Título II de la Constitución, pues en un Estado social de derecho y democrático no existen derechos absolutos.[3]

Ley 44 de 1993 Régimen Común sobre Derecho de Autor y Derechos Conexos.[4]

Ley 232 de 1995: aprobada el 26 de diciembre de 1995. Por medio de la cual se dictan normas para el funcionamiento de los establecimientos comerciales, fue derogada el 29 de enero de 2017 por la Ley 1801 de 2016.

Ley 527 de 1999: aprobada el 18 de agosto de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales[5], y se establecen las entidades de certificación y se dictan otras disposiciones, ha sido modificada por el Decreto 19 de 2012 y declarada EXEQUIBLE.[6]

---

[3] Colombia. Constitución Política de Colombia de 1991

[4] DELITOS INFORMATICOS. [Consulta: 31 de agosto del 2022]. [Página Web]. Disponible en: https://1library.co/document/q76wroky-delitos-informaticos-y-marco-normativo-en-colombia.html

[5] Informática Jurídica. Legislación Informática de Colombia. [Consulta: 31 de agosto del 2022]. [Página Web]. Disponible en: https://www.informatica-juridica.com/legislacion/colombia/

[6] UNIVERSIDAD DE COLOMBIA. Ingeniería de servicios por Internet. . [Consulta: 31 de agosto del 2022]. [Página Web]. Disponible en: https://osbraghe1826.wordpress.com/correo-electronico

Ley 545 de 1999: aprobada. "Tratado de la OMPI Organización Mundial de la Propiedad Intelectual- sobre Interpretación o Ejecución y Fonogramas (WPPT)", adoptado en Ginebra el 20 de diciembre de 1996,

A partir del año 2000 se generaron leyes asociadas a la protección de la información:

Ley 565 de 2000: Aprobada el 2 de febrero de 2000. Por medio de la cual se aprueba el "Tratado de la OMPI Organización Mundial de la Propiedad Intelectual-- sobre Derechos de Autor (WCT)", adoptado en Ginebra, el 20 de diciembre de 1996, dicha Ley es declarada EXEQUIBLE por la Corte Constitución al mediante Sentencia C 1183-- 00 de 13 de septiembre de 2000.

Ley 588 de 2000: Aprobada en el 2000. En ella se reglamenta el ejercicio de la actividad notarial, promulgada por el por el Congreso de la República.[7]

594 de 2000: Se aprobó en el 2000. Se crea la ley general de archivos y se dictan otras disposiciones, en la actualidad esta ley está vigente en el territorio nacional.

Ley 599 de 2000: Aprobada en el 2000. Por la cual se crea el Código Penal, esta ley ha sido efecto de modificación desde su publicación, modificaciones realizadas: la Ley 1787 de 2016, Ley 1819 de 2016, Ley 1850 de 2017, Ley 1908 de 2018, Ley

[7]DELITOS INFORMÁTICOS Y MARCO NORMATIVO EN COLOMBIA. [Consulta: 31 de agosto del 2022]. [En línea]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/28115/%20%09jparraca.pdf

451915 de 2018, Ley 1918 de 2018 y la Ley 890 de 2004, a pesar de las modificaciones esta Ley está vigente en el territorio colombiano[8].

Ley 679 de 2001: Aprobada el 3 de agosto de 2001. Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución, la Ley está vigente en la actualidad y ha sido modificada por la Ley 1101 de 2006, Ley 1336 de 2009 y la Ley 1801 de 2016.

Ley 719 de 2001: aprobada en el 2001. Allí se actualizan las Leyes 23 de 1982 y 44 de 1993 y se dictan otras disposiciones.

Ley 890 aprobada en el 2004. Por la cual se modifica y adiciona el Código Penal, ley declarada EXEQUIBLE por la Corte Constitucional mediante Sentencia C de 3 de marzo de 2005.[9]

Luego, desde el 2006 siguió así:

Acuerdo No. PSAA063334 de 2 de marzo de 2006 del Consejo Superior de la Judicatura, por el cual se reglamentan la utilización de medios electrónicos e informáticos en el cumplimiento de las funciones de administración de la justicia (Vigente).[10]

---

[8]Sistema de medios públicos. Leyes. https://www.rtvc.gov.co/quienes-somos/leyes [Consulta: 31 de agosto del 2022]. [En línea]. Disponible en: https://www.rtvc.gov.co/quienes-somos/leyes

[9] Informática Jurídica. Legislación Informática de Colombia. [Consulta: 31 de agosto del 2022]. [Página Web]. Disponible en: https://www.informatica-juridica.com/legislacion/colombia/

[10] DELITOS INFORMATICOS. [Consulta: 31 de agosto del 2022]. [Página Web]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/28115/%20%09jparraca.pdf

Desde el 2009 se busca tener un mayor avance legislativo generando decretos, resoluciones y leyes, destacando claro está, la ley 1273 que marco la diferencia:

Ley 1273 de 2009

En el año 2009 se creó una ley dentro del margen legal colombiano para proteger los sistemas de información de delitos informáticos, es la ley 1273 del 5 de enero de 2009 donde se plasman varias infracciones de índole informático para aquellos casos donde haya conductas que puedan ser sancionadas por su carácter ilícito o criminal, un ejemplo de ello es lo podemos ver en su artículo 269 de los numerales a al j.

"…Artículo 269A: Acceso abusivo a un sistema informático.
"Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación." ("Artículo 269B: Obstaculización ilegítima de sistema informático o red ...")
Artículo 269C: Interceptación de datos informáticos.
Artículo 269D: Daño Informático.
Artículo 269E: Uso de software malicioso.
Artículo 269F: Violación de datos personales.
"Artículo 269G: Suplantación de sitios web para capturar datos personales." ("Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR ... - Blogger")
Artículo 269I: Hurto por medios informáticos y semejantes.
Artículo 269J: Transferencia no consentida de activos…"[11]

[11] DELITOS INFORMÁTICOS EN COLOMBIA. LEYES, PENAL. julio 26 de 2019. [Consulta: 30 de agosto del 2022]. [En línea]. Disponible en: https://www.notaria19bogota.com/delitos-informaticos-en-colombia

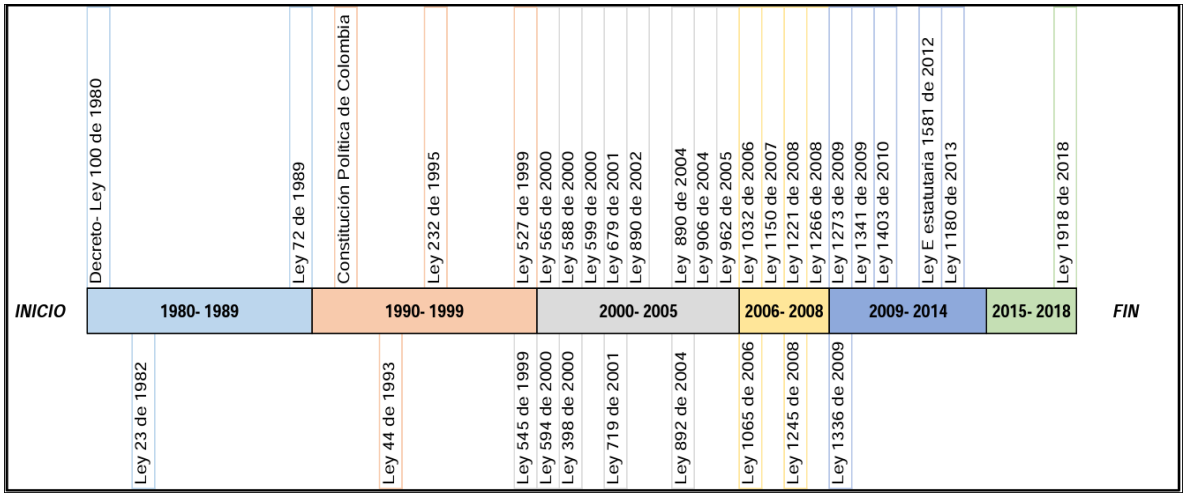
Ley 1403 aprobada en el 2010, por la cual se adiciona la Ley 23 de 1982, sobre derechos de autor, se establece una remuneración por comunicación pública a los artistas intérpretes o ejecutantes de obras y grabaciones audiovisuales o "Ley Fanny Mikey".[12]

Decreto 2573 de 12 de diciembre de 2014, por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

Desde el 2015 se incorporan con más fuerza decretos y leyes asociados a los delitos informáticos, entre ellos:

Ley 1918 de 24 de julio de 2018, "Convenio sobre la Ciberdelincuencia".

Ilustración 1. Línea de tiempo



Fuente. Mónica María Jiménez. Conoce el Marco de Ciberseguridad del NIST (National Institute of Standards and Technology). en línea. Medellín - Antioquía. Disponible en: https://www.piranirisk.com/es/blog/marco-ciberseguridad-nist-que-es

[12] Informática Jurídica. Legislación Informática de Colombia. [Consulta: 31 de agosto del 2022]. [Página Web]. Disponible en: https://www.informatica-juridica.com/legislacion/colombia/

2.2 Pruebas de pentesting

Para poder nombrar las etapas del pentesting, debemos conocer el significado de pentesting y las clases de este.

El pentesting en realidad es un ataque simulado dentro de un entorno controlado donde podremos analizar y detectar falencias y posibles huecos de seguridad dentro de la organización, realizando un informe completo para que los directivos puedan tomar la mejor decisión y corregir las fallas encontradas.

Tenemos tres clases de pentesting

- **Test de Caja Blanca**: este tiene toda la información los sistemas informáticos de la empresa como la infraestructura, datos, IP, logings, contraseñas, Fireworks, etc. Esta prueba es el más completo ya que con los datos recolectados las pruebas serán suficientemente certeras para descubrir los huecos de seguridad o fallos y poder indicar las acciones que deban tomarse.

- **Test de Caja Negra**: En esta prueba no se tiene ningún dato de la empresa y empieza desde ceros, haciendo que la prueba se vea real ya que al no tener información se actuaría como si fuera un ciberdelincuente real porque va a ciegas haciendo pruebas en la estructura de la empresa. Esta prueba es interesante ya que se reconocerán las debilidades de los sistemas, aplicaciones y red.

- **Test de Caja Gris**: este tiene la información parcial de las aplicaciones y sistemas de la empresa, por lo tanto, se puede decir que es la mezcla entre la prueba blanco y negro. Se trabaja con muy poca información lo que implica gastar tiempo y recurso para realizar la identificación de debilidades, huecos de seguridad y amenazas.

Estos tipos se utilizan teniendo en cuenta los requerimientos del cliente y de la información que se tenga.

Métodos más utilizados en el Pentesting:

ISAAF: Con este método el ataque se realiza en base a información previamente organizada de acuerdo con unos parámetros establecidos por el grupo de expertos.

PCI DSS: Este método lo utilizan mucho las instituciones públicas o privadas que se dedican al procesamiento, almacenamiento y transmisión de datos bancarios o movimientos transacciones en el comercio.

PTES: Este método es usado casi siempre que se inicia un pentesting, es muy recomendado.

OSSTMM: Es un manual para facilitar la realización de auditorías de seguridad de forma más eficiente y acertada.

Para realizar un buen pentesting se requieren las siguientes etapas:

- **Recopilar información**: en esta fase se buscan datos de la empresa de cualquier clase de fuente que muestre información: redes sociales, blogs, fotos, etc.

- **MATELGO**: Es una herramienta que permite de manera sencilla y automatizada, levantar información relacionada al objetivo. Él es OSINT (Open Source Intelligence), o sea, él recolecta datos de fuentes disponibles al público. Es de destacar la cantidad de información que se puede

recolectar. Además, puede mostrar de manera gráfica cómo se relacionan esas informaciones[13].

- **Búsqueda de una base técnica**: Se buscan los recursos, aplicaciones y medios con los que cuente la empresa.

  Las herramientas más utilizadas para esta etapa son:

- **NMAP:** Permite la ejecución de scripts personalizados que permiten la identificación de informaciones específicas. El NMAP realiza un escaneo de los objetivos tales como redes y hosts, estén abiertos a internet o no. Además, escanea puertas de servicios que están abiertas, determina el tipo de servicio, versión y posibles sistemas operacionales, se hace un barrido de red y se obtienen respuestas de todos los dispositivos que están conectados.

- **Análisis de vulnerabilidades y amenazas**: En esta fase una de las más importantes se empezará a buscar y encontrar vulnerabilidades, huecos de seguridad, errores en la red, aplicaciones de seguridad que no funcionen y cualquier clase de problema que se pueda estar presentando que genere un problema de seguridad para la infraestructura y los sistemas de información de la empresa.

- **METASPLOIT**: una herramienta poderosa que cuenta con un conjunto de módulos para investigar y explorar debilidades en muchos sistemas, aplicaciones y sistemas operacionales entre otros.

---

[13] Osctec. Pentest: las 10 mejores herramientas usadas en el mercado. 2022. [Consulta: 09 de octubre del 2022]. [Página Web]. Disponible en: https://ostec.blog/es/aprendizaje-descubrimiento/pentest-las-10-mejores-herramientas-usadas-en-el-mercado/

Su objetivo es proveer un ambiente de búsqueda de explotación de vulnerabilidades. Después de identificar las debilidades se realiza la ejecución del exploit, aplicando técnicas de ingeniería inversa o programación. De esa manera el exploit es ejecutado en varios ambientes, probando la existencia de debilidades[14].

- **Operación y procesamiento de datos:** En esta fase se simularán los ataques en escenarios controlados y necesarios para conseguir información y poder obtener el reporte de las vulnerabilidades a los que están expuestos.

- **Generación de reportes o informes**: En esta fase que será la final, se presentan los resultados de la simulación que se concluyó con la información lo más completa posible incluyendo las propuestas para mitigar, corregir, solucionar fallos de seguridad.

2.3 Herramientas de Ciberseguridad

En el trabajo de un buen pentesting todas las herramientas de ciberseguridad cobran vital importancia que podemos expandir más las posibilidades de llegar análisis profundo y con criterio, entre algunas herramientas encontramos:

Metasploit

es un software de código abierto muy completa que sirve para realizar y reproducir exploits continuos contra una máquina remota buscando errores en la seguridad de esta, fue creado originalmente en lenguaje de programación Perl, pero luego fue totalmente reescrito en lenguaje Ruby. Una de las ventajas más grandes es que es

[14] Osctec. Pentest, todo lo que debe saber. 25 de mayo 2022. [Consulta: 09 de octubre del 2022]. [Página Web]. Disponible en: https://ostec.blog/es/seguridad/pentest-todo-lo-que-debe-saber/

un programa multiplataformas y gratuito, aunque claro tiene su versión paga que actualiza diariamente los exploits.

Con el Metasploit podemos:

- Escanear y recopilar toda la información de una máquina
- Identificación y explotación de vulnerabilidades
- Escalamiento de privilegios y robo de datos
- Instalación de una puerta trasera
- Fuzzing - conjunto de pruebas de test caja negra que permiten descubrir fallos en las aplicaciones la introducción de datos al azar, inválidos y malformados
- Escapar del antivirus
- Eliminación de registros y trazas

Nmap

Es una herramienta utilizada para exploración o escaneo de redes y puertos, para identificar servicios en ejecución, detectar sistemas operativos y para ejecución de auditorías entre otras, es software de código libre diseñado para realizar un análisis rápido y efectivos en redes ya sean pequeñas o grandes[15].

Estos son algunos de los Tipos de escaneos al azar más utilizados por NMAP:

La existencia de los CVE no implica que el fallo sea necesariamente un daño para toda una infraestructura o que no tenga arreglo hay, por lo tanto, niveles de riesgo que podemos decir no impactara tanto en la empresa y tiene soporte y arreglo.

[15] Osctec. Pentest: las 10 mejores herramientas usadas en el mercado. [Consulta: 09 de octubre del 2022]. [Página Web]. Disponible en: https://ostec.blog/es/aprendizaje-descubrimiento/pentest-las-10-mejores-herramientas-usadas-en-el-mercado/

- **Escaneo Ping / Escaneo ARP**: Utilizados para conocer qué servidores se encuentran activos ejecutando un escaneo ARP para obtener información de dichos servidores.

- **Sondeo de lista**: Se realiza un valor inverso de DNS para obtener los nombres de los equipos de la red, con este escaneo no se envía ningún tipo de paquete hacia el objetivo a diferencia del escaneo Ping.

- **Escaneo TCP connect**: Realiza una conexión completa con los puertos que están a la escucha (3 way hand shake). Es el escaneo por defecto sino se utilizan privilegios de administrador para ejecutar el TCP SYN.

Es de tener en cuenta que NMAP tiene una fortaleza y flexibilidad por los scripts que maneja ya que su motor de scripting (NSE), por otro lado, es de destacar que es una de las mejores guías para ayudar a encontrar vulnerabilidades y mantener control de una red, detectando cualquier acceso no autorizado.

OpenVas

Es una herramienta de escáner de vulnerabilidades de fácil manejo, multiplataforma con aplicación web que puede detectar problemas en todo tipo de equipo, dispositivos o redes de empresas pequeñas o grandes clasificando las vulnerabilidades como de riesgo alto (que representa de color rojo) y que requieren atención inmediata, riesgo medio que representa de color amarillo y que requieren atención a corto plazo y riesgo bajo que no requieren atención inmediata.

Esta herramienta cuenta con varias opciones de escaneo, entre ellas:

“Pruebas autenticadas y no autenticadas.

Protocolos industriales y de Internet de alto y bajo nivel.
Ajustes personalizados de rendimiento para exploraciones a gran escala.
Desarrollado en un potente lenguaje de programación interno para implementar cualquier tipo de prueba de vulnerabilidad."[16]

Por otro lado, se deben destacar las características que tiene y que ayudan a que su trabajo se realice exitosamente.

- Documentación extensa y definida.

- Posibilidad desde línea de comandos y en modo gráfico con una interfaz con utilidades y repleta de datos de interés, capaz de sacar informes de interés.

- Una comunidad que ofrece bastante tutoriales y apoyo a la hora de explotar vulnerabilidades, por su web y por otros foros como Reddit, por ejemplo.

Servicios en línea:

ExploitDB

Es un directorio donde se muestran las vulnerabilidades de aplicaciones y como beneficiarse de ellas, mostrando explicaciones específicas. Estas bases pueden ser de gran ayuda para las personas que deseen aprender, pero también pueden hacer mucho daño si no se saben tratar.

En esta página https://www.exploit-db.com podemos encontrar la base de datos actualizada con lo que los usuarios van cargando.

[16] openwebinars. . [Consulta: 09 de octubre del 2022]. [Página Web]. Disponible en: https://openwebinars.net/blog/que-es-openvas/

CVE

Son listas de vulnerabilidades de seguridad de toda la información, estas fallas vienen identificadas con un numero asignado previamente que se divulga públicamente. Estos listados se actualizan diariamente y un insumo importante al momento de realizar verificaciones por parte de los especialistas de seguridad para encontrar vulnerabilidades, fallos o huecos de seguridad y saber cómo actuar ante estas.

La numeración de las fallas o su identificador es asignada por CNA, quienes tienen a su cargo esta tarea, hay que tener en cuenta que en este momento hay muchos CNA que representan a proveedores de TI, Instituciones de investigación, empresas dedicadas a seguridad informática entre otros.

2.4 Escenario 1 – Banco De Trabajo

Los siguientes son los pasos que seguiremos:

• **P**aso **A**: descargar la herramienta virtualizadora "**VirtualBox**" en su última versión.

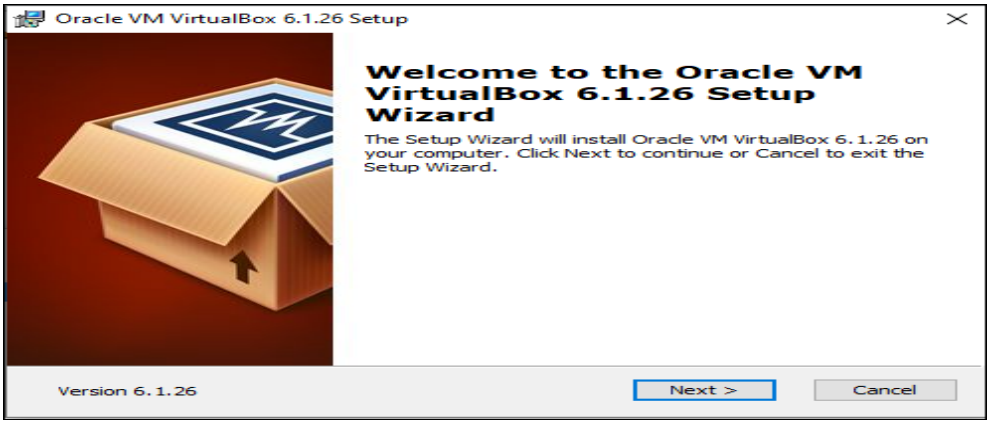
Descargar la herramienta virtualizadora "VirtualBox" en su última versión.

1. Descargar e instalar una máquina virtual - VirtualBox o VMware Player

Ilustración 2. Instalación máquina virtual

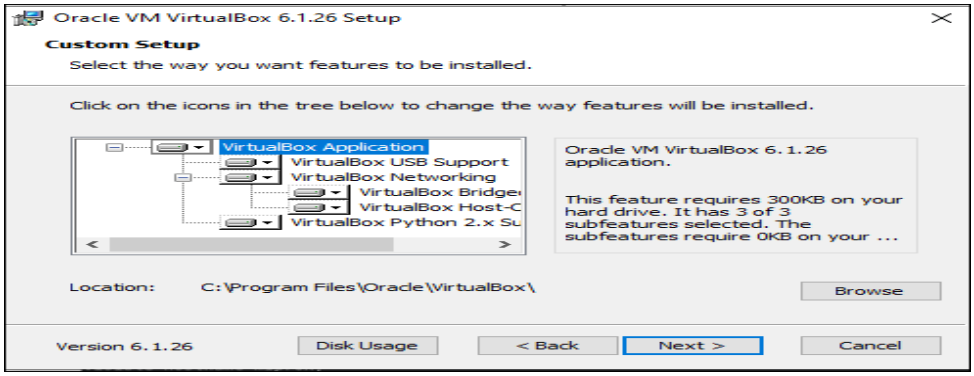
Descarga desde la página https://www.virtualbox.org/wiki/Downloads y seleccionamos la versión que deseamos descargar

Ilustración 3. Se realiza el paso a paso solicitado por el programa



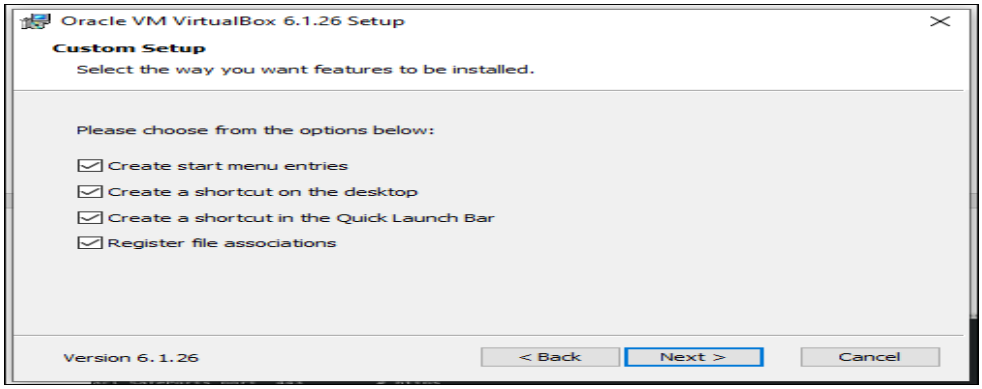
Fuente propia

Ilustración 4. Selección de disco de instalación



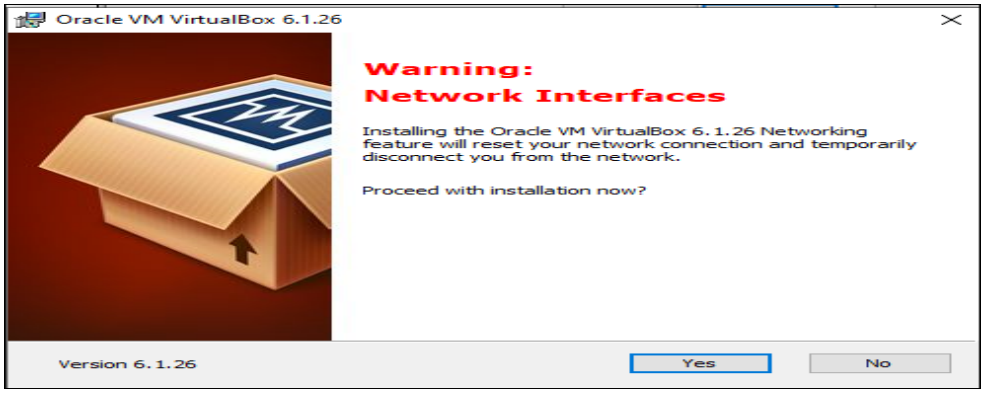
Fuente: propia

Ilustración 5. Creación de lugares de vista del programa



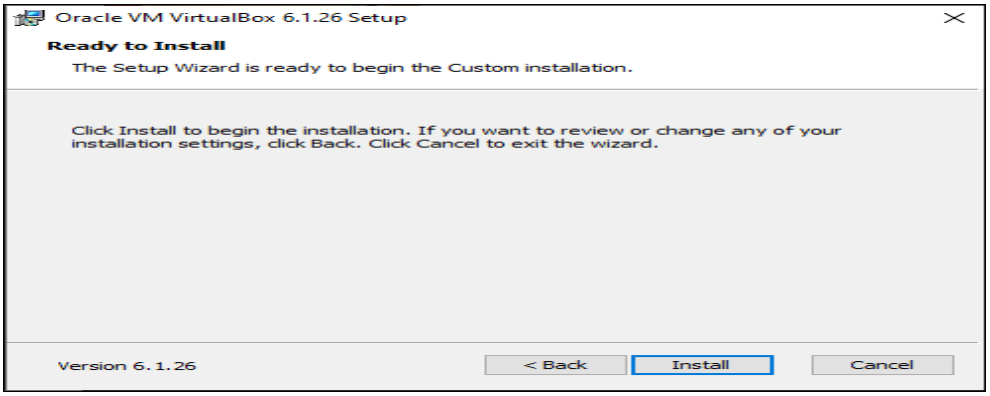
Fuente: propia

Ilustración 6. Finalizamos con la autorización de instalación



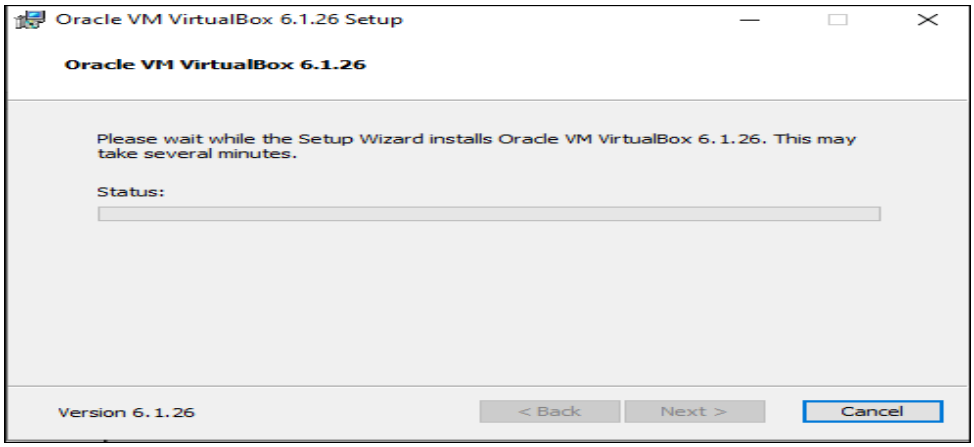
Fuente: propia

Ilustración 7. Aceptamos e instalamos



Fuente: propia

Ilustración 8. Proceso de instalación



Fuente: propia

Ilustración 9. Instalación realizada y máquina virtual lista para trabajar

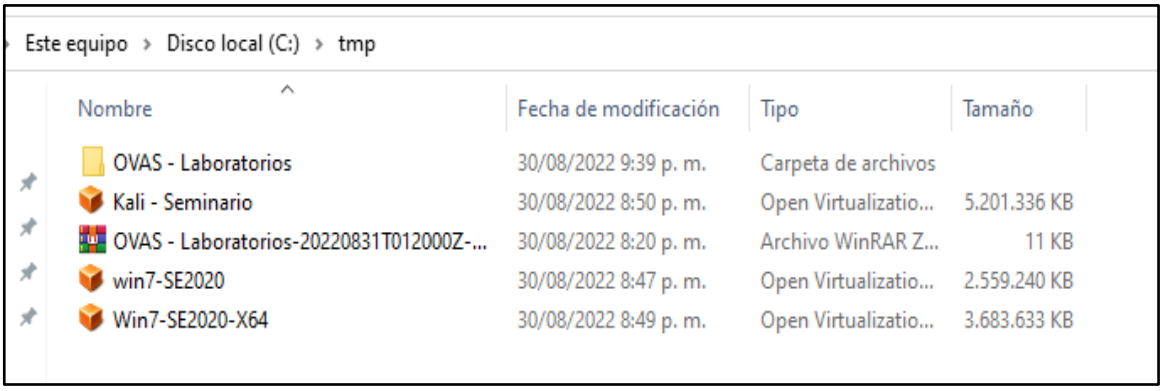
Fuente: propia

• **Paso B**: descargas de un **Windows** 7 x86, un **Windows** 7 x64, un **Kali Linux**.

Ilustración 10. Descarga de los OVAS para el laboratorio

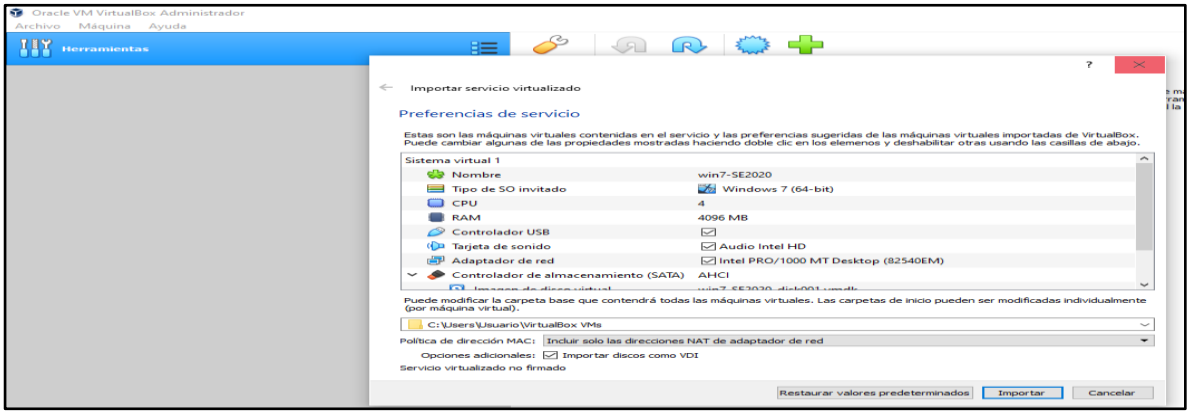
Fuente: propia

Ilustración 11. Descarga exitosa de los OVAS



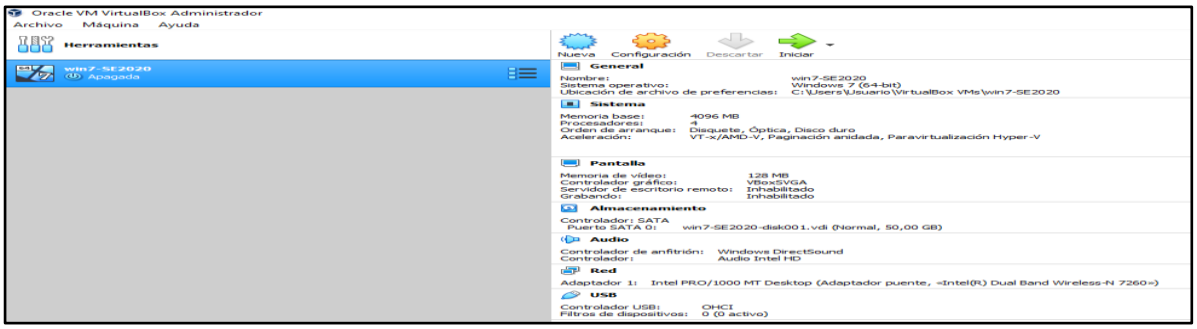
Fuente: propia

Ilustración 12. Montaje de la máquina virtual denominada WIN7-SE2020



Fuente: propia

Ilustración 13. Creación exitosa de la máquina virtual denominada WIN7-SE2020

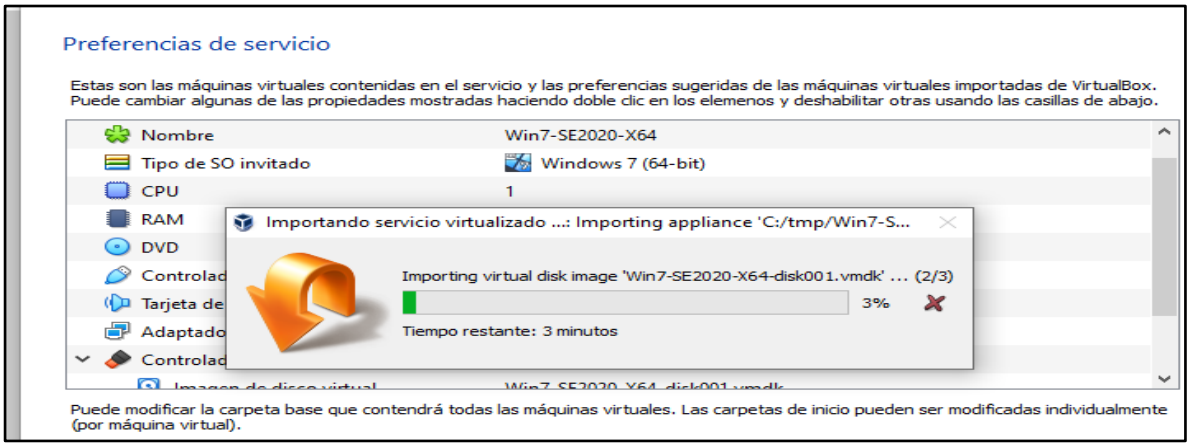


Fuente: propia

Ilustración 14. Montaje de la máquina virtual denominada WIN7-SE2020-X64

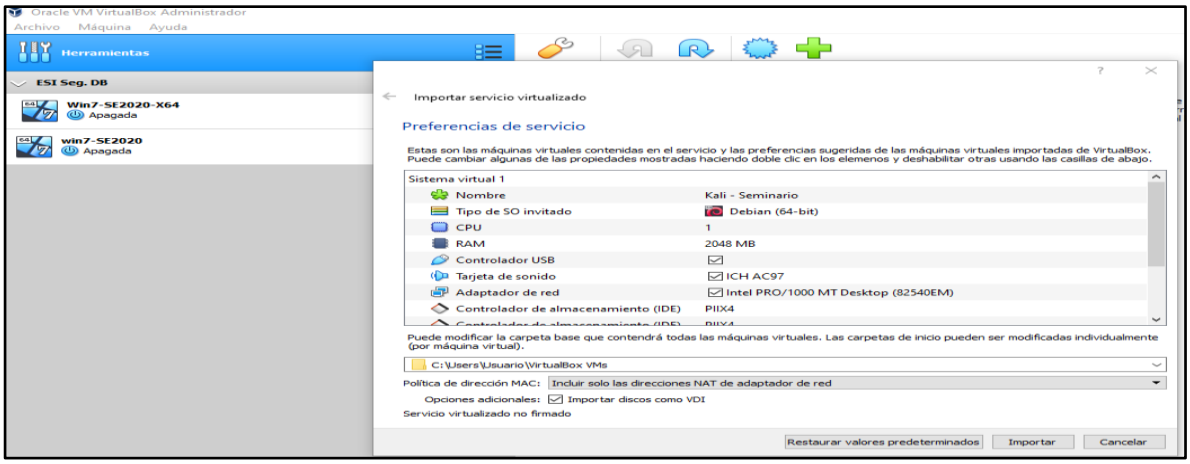
Fuente: propia

Ilustración 15. Creación exitosa de la máquina virtual denominada WIN7-SE2020



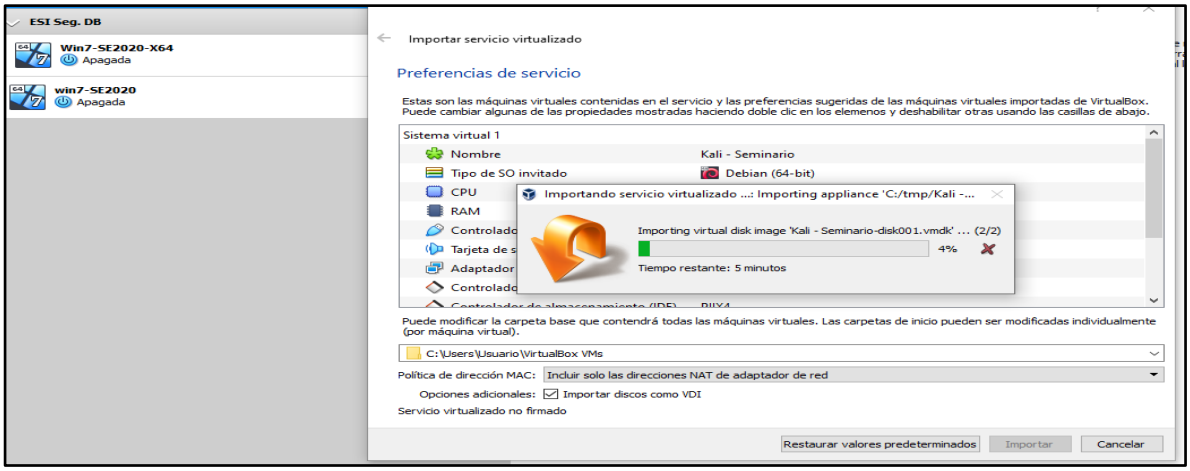
Fuente: propia

Ilustración 16. Montaje de la máquina virtual denominada Kali - Seminario



Fuente: propia

Ilustración 17. Creación exitosa de la máquina virtual denominada Kali - Seminario



Fuente: propia

Se finaliza el montaje de las máquinas virtuales del laboratorio

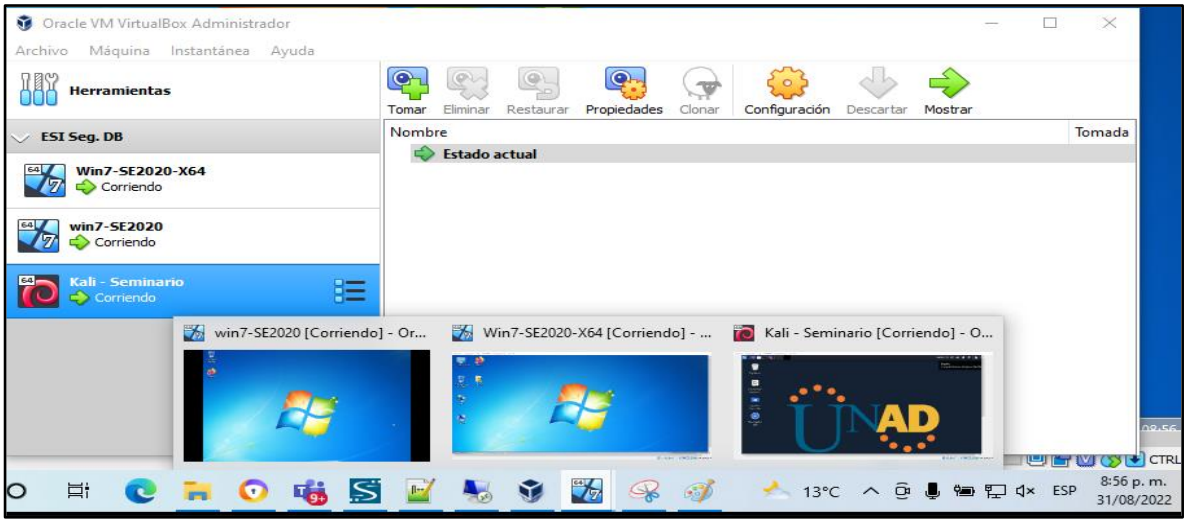
Ilustración 18. Máquinas correctamente instaladas

Fuente: propia

Paso **C**: validación de comunicación de cada una de las máquinas.

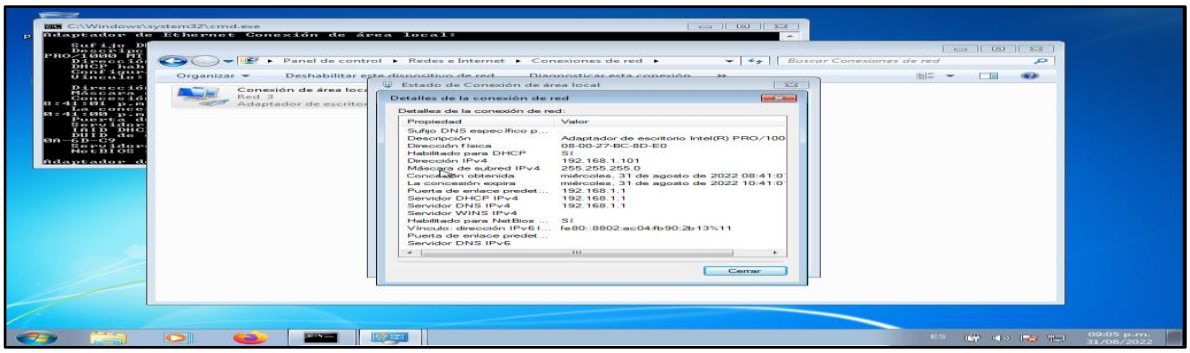
Se encienden las máquinas virtuales, teniendo en cuenta que primero se encienden las de Windows y por último Kali Linux.

Ilustración 19. Máquinas del laboratorio encendidas.



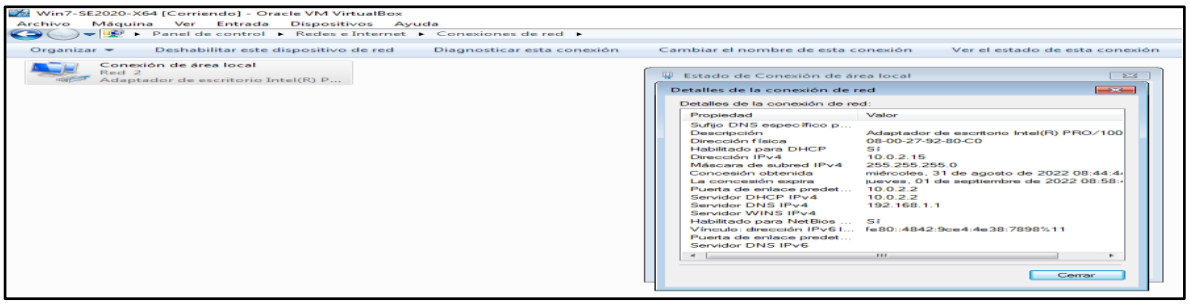
Fuente: propia

Ilustración 20. Validación de IP por defecto de la máquina virtual WIN7-SE2020.



Fuente: propia

Ilustración 21. Validación de IP por defecto de la máquina virtual WIN7-SE2020-X64.



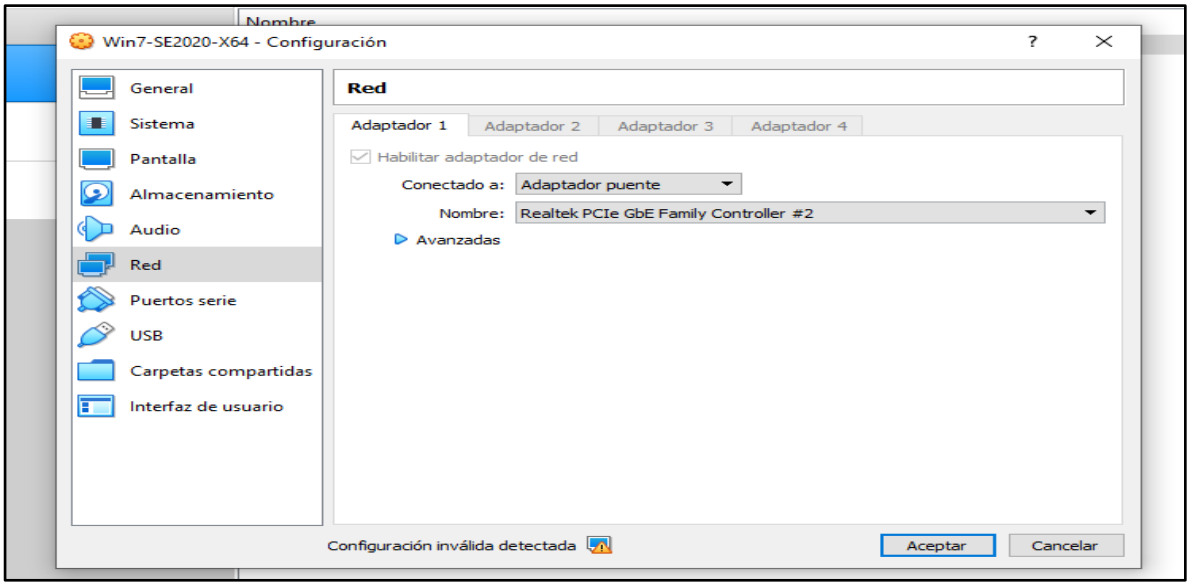
Fuente: propia

Ilustración 22. Validación de IP por defecto de la máquina virtual Kali-Seminario

Fuente: propia

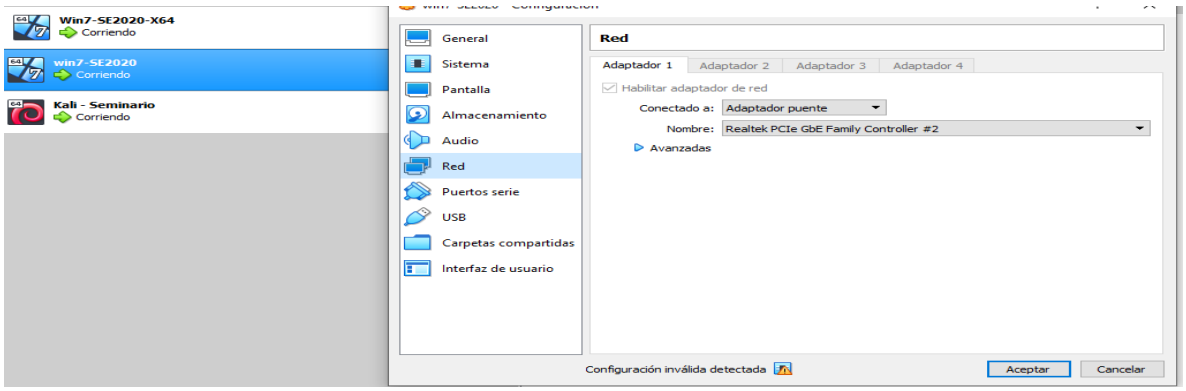
Luego de la verificación de la IP por defecto, vamos a cada maquina y configuramos las características del adaptador de red para lograr que las tres máquinas queden dentro de la misma red.

Ilustración 23. Configuración del adaptador de red Win7-SE2020-X64



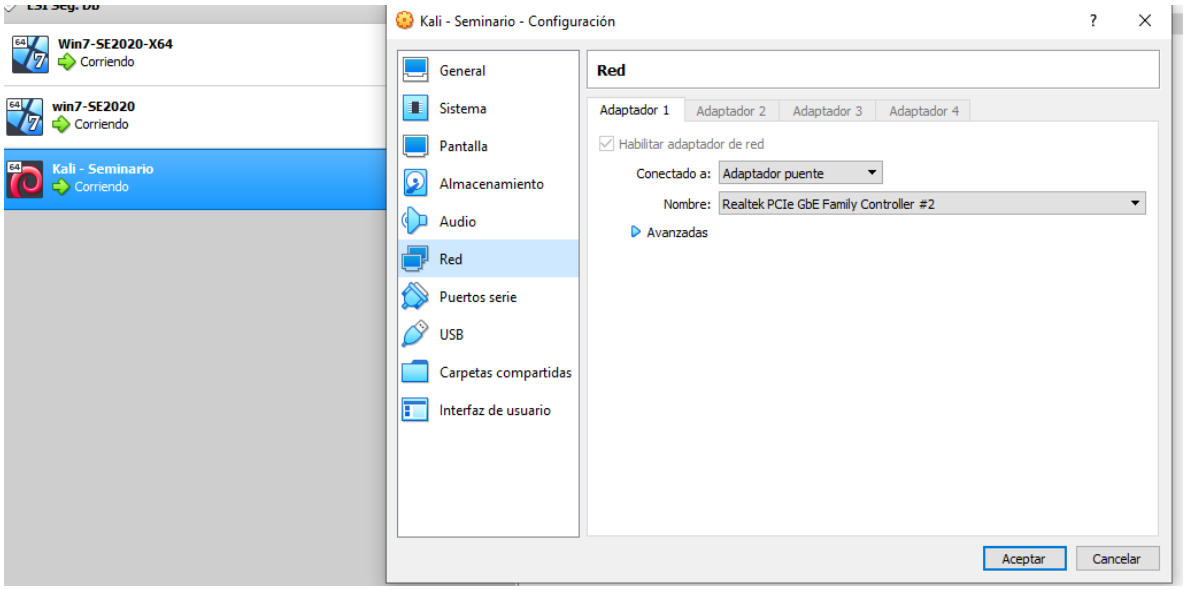
Fuente: propia

Ilustración 24. Configuración del adaptador de red Kali - Linux



Fuente: propia

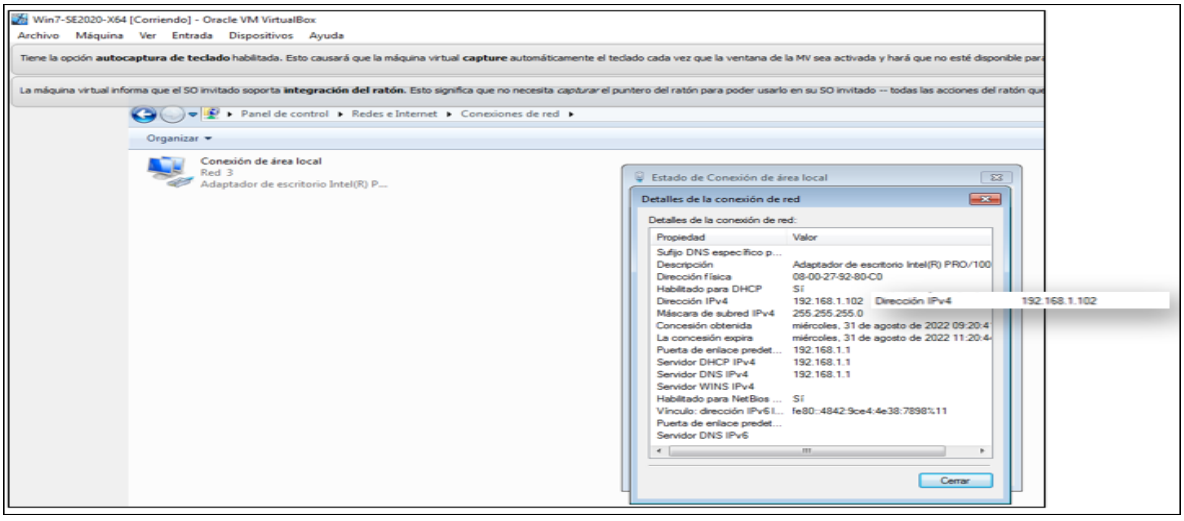
Ilustración 25. Configuración del adaptador de red Win7-SE2020



Fuente: propia

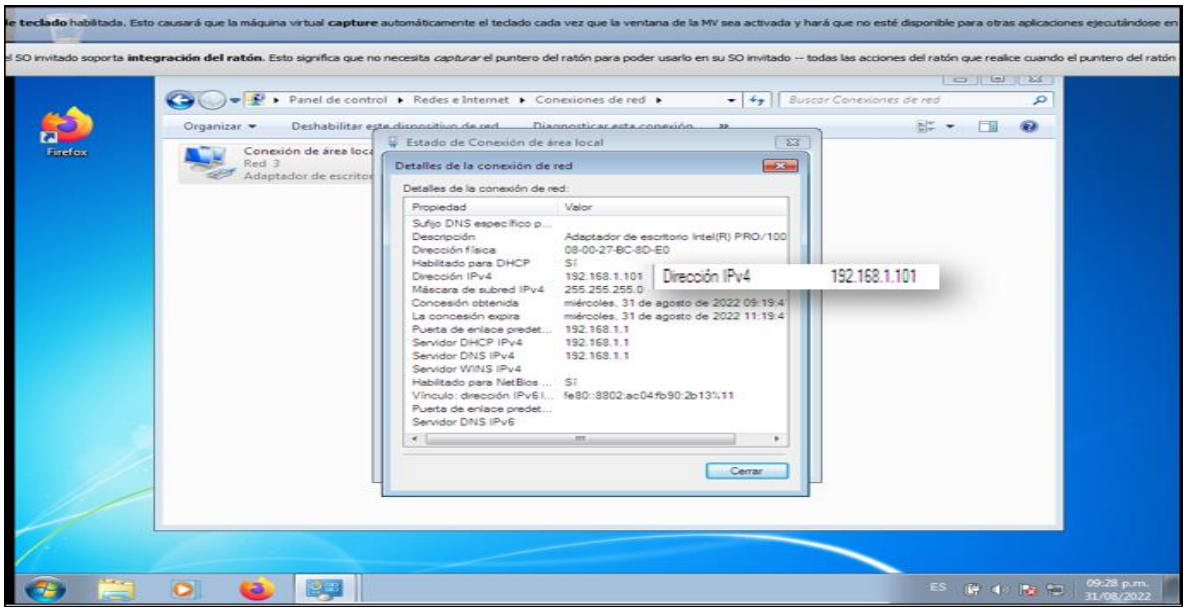
Luego de configuradas los adaptadores de red de las maquinas se procede a validar que hayan quedado dentro del mismo segmento de red.

Ilustración 26. Verificar la dirección IP Win7-SE2020-X64



Fuente: propia

Ilustración 27. Verificar la dirección IP Win7-SE2020-X64



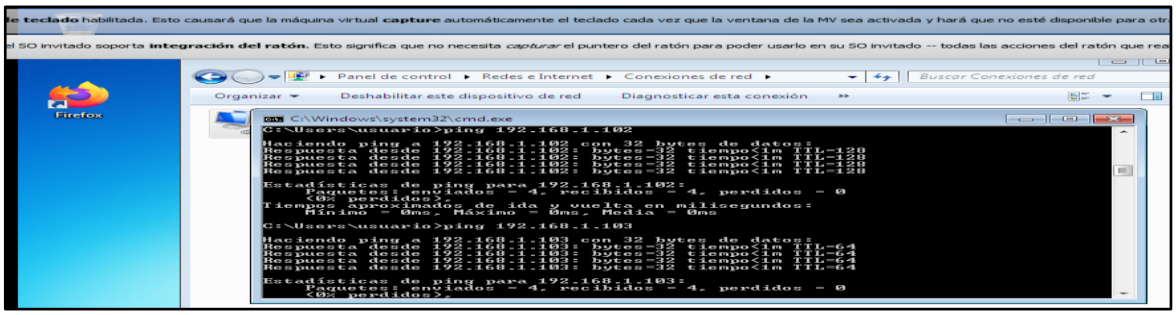
Fuente: propia

Ilustración 28. Verificar la dirección IP Win7-SE2020-X64

Fuente: propia

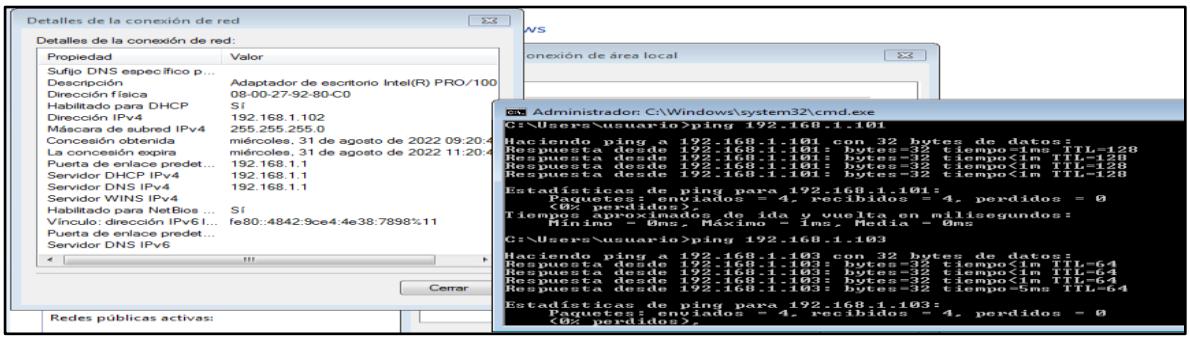
Por último, se valida la comunicación entre las máquinas realizando el ping correspondiente.

Ilustración 29. Ping desde win7-SE2020 a las maquinas win7-SE2020-X64 y Kali-Seminario



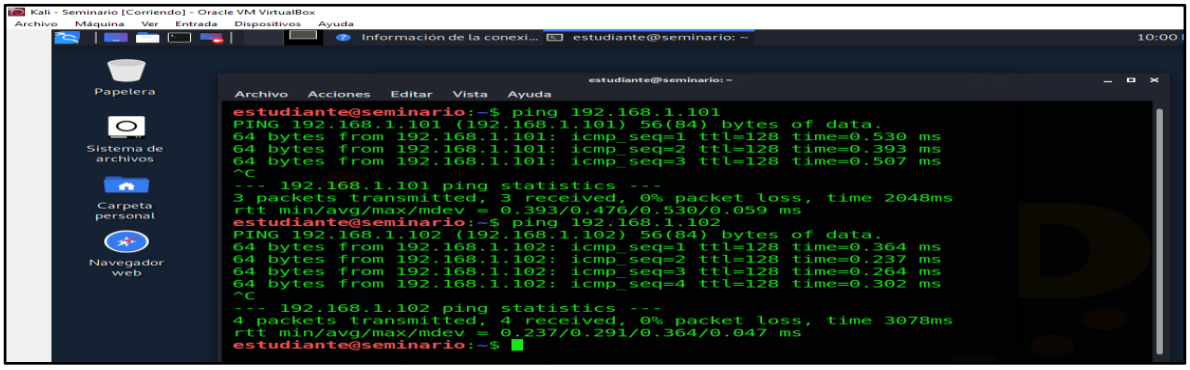
Fuente: propia

Ilustración 30. Ping desde win7-SE2020-X64 a las maquinas win7-SE2020 y Kali-Seminario



Fuente: propia

Ilustración 31. Ping desde Kali-Seminario a las maquinas win7-SE2020-X64 y win7-SE2020



Fuente: propia

3. ETAPA 2 - PROCESOS ILEGALES Y NO ETICOS

3.1 Procesos Ilegales

Al revisar el documento de forma general siempre debe revisarse punto por punto buscando que no irregularidades, sin embargo, se encuentran algunas irregularidades en el acuerdo de confidencialidad que nombrare más adelante. Es evidente que el ex abogado de HACKERS SECURITY que realizó el documento no lo hizo de buena fe y está atentando contra la buena imagen de la empresa haciendo incurrir en delitos a la empresa.

3.2 Que hacer en caso de encontrar procesos ilegales

Al leer el documento detallamente, se encuentra las posibles irregularidades en el acuerdo de confidencialidad, así:

Primero la alta gerencia de la organización Hackers Security no debió hacer entrega de un contrato sin ser revisado minuciosamente teniendo el conocimiento de que fue elaborado por un exfuncionario que fue despedido por encontrar algunos procesos ilícitos en su contra. Es un error que puede costarle la reputación, la confiabilidad y el reconocimiento adquirido a nivel mundial.

> **“Primera. Objeto**: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o ***sobre procesos ilegales dentro de Hackers Security no podrán ser divulgados***.”.

En el objeto del acuerdo anteriormente mencionado se encuentra citado literalmente "…***procesos ilegales dentro de Hackers Security…***". Lo cual indica una expresa violación de los artículos:

- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación[17].

- Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere en su numeral 3: Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este[18].

- En su numeral 7. Utilizando como instrumento a un tercero de buena fe.

Numeral 2: Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, **datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos**".

---

[17] COLOMBIA. CONGRESO DE LA REPBLICA. Ley 1273 de 2009. "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. [En línea].Bogotá D.C., Diario Oficial. 2009. 47.223 Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.enticconfio.gov.co/images/stories/normatividad/Ley_1273_de_2009%20.pdf

[18] Policía Nacional. Normatividad sobre delitos informáticos. 2022. [Consulta: 08 de octubre del 2022]. [Página Web]. Disponible en: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

El numeral 2 cita: "…***datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos***…".

En este caso y revisando la ley 1276 de 2009 podemos constatar que se podría incurrir en los siguientes:

- Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO, ya que solicitan no divulgar el acceso abusivo a un sistema de información.

- Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS.

En clausula 4 las obligaciones de la parte receptora, en sus numerales 3 : " ***No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de*** terceros." y 4: "***Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas***.".

En estos numerales podemos ver claramente que podía existir una violación a toda la ley 1276 de 2009 ya que incurre en todos los delitos a los cuales hace referencia esta ley.

Numeral 7: "***Responder por el mal uso que le den sus representantes a la información confidencial***. "

Este numeral podría decirse que es violatorio no solo de esta ley sino también sobre todas las leyes que protejan al contratado, ya que él no tiene la obligación en ningún caso de responder por el mal uso de la información confidencial del contratante.

Analizando se tomaría el siguiente artículo en específico de ley 1276 que se estaría violando. Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA, numeral 7: Utilizando como instrumento a un tercero de buena fe.

Numeral 9. La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de Hackers Security.

Al igual que en el objeto la posible violación al Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.

Y al artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere en su numeral 3: Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este[19].

Octava. Solución de controversias: Las partes *(nombre estudiante – nombre empresa)* se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** ***En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un***

[19] COLOMBIA. CONGRESO DE LA REPBLICA. Ley 1273 de 2009. "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. [En línea].Bogotá D.C., Diario Oficial. 2009. 47.223 Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.enticconfio.gov.co/images/stories/normatividad/Ley_1273_de_2009%20.pdf

abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Hackers Security.

Nuevamente encontramos que hay solicitud de no informar de procesos ilegales en este documento, lo cual ya indica que no fue escrito con errores, sino que el ex abogado sabía lo que desea imprimir en el acuerdo, por tanto, para mi este numeral podría decirse al igual que el numeral 7, que es violatorio no solo de esta ley sino también sobre todas las leyes que protejan al contratado, ya que él no tiene la obligación en ningún caso de responder por el mal uso de la información confidencial del contratante.

3.3 Aplicar a trabajo con la empresa

Cuando se lee el acuerdo que **Hackers Security** entrega a las personas que desean trabajar con ellos y al encontrar tantas irregularidades en sus cláusulas donde visiblemente atentan contra la ética no solo personal, sino profesional como vemos en uno de sus apartes del Objeto:

"…*se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre* ***procesos ilegales*** *dentro de Hackers Security no podrán ser divulgados*…".

La ética personal y profesional no debe permitir trabajar con esta clase de empresas, porque durante la vida en todos los aspectos tanto personal, académica y laboral siempre me he considerado una persona responsable, honesta y transparente, no podría ver que haya irregularidades y no denunciarlas ante los entes de control pertinentes.

Otro caso totalmente inaceptable para mi es que en el acuerdo soliciten explícitamente no denunciar: "…***Abstenerse de denunciar*** *y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas*...". Esto quiere decir, que si se firma el acuerdo y se acepta trabajar con la empresa estaremos aceptando que vamos a encontrar actividades ilegales y que no vamos a poder denunciar, tendremos que mirar para otro lado y decir "aquí no está pasando nada" y realmente no debería ser el objetivo de la carrera.

Podríamos quedarnos nombrando muchas más irregularidades y propuestas de actitudes deshonestas, por lo tanto, no me arriesgaría a trabajar con ellos, ya que muy seguramente mi nombre y mi trabajo se verían seriamente afectados por sus acciones y exigencias. Mi trabajo debe tener una reputación excelente para aplicar a compañías de alto nivel. Sinceramente el sueldo podría decirse que es bueno, pero no vale manchar mi hoja de vida sin razón.

3.4 Operación Andrómeda Buggly

Al realizar la investigación sobre la "OPERACIÓN ANDROMEDA BUGGLY" encontré que consistía en una fachada del Ejecito Nacional para hacer sus operaciones de inteligencia.

En la ciudad de Bogotá, en el barrio de galerías se ubicó un local al que llamaron "***Buggly Ethical Hacking***" y que lideraba el sr. Llamado "Bender", la idea principal era tener un espacio para los interesados en el tema, el sr. Bender llego a promocionarlo en todas las redes sociales y blogs que encontraba sobre Ethical Hacking cumpliendo su objetivo, puesto que hubo muchas personas conocedoras del tema que se interesaron en el sitio.

Según los informes la idea principal de este local era llamar a conocedores en seguridad informática y armar una gran comunidad. En este sitio empezaron a reunirse para realizar diferentes actividades de seguridad, compartían diferente información, conocimiento y también ponían juegos de retos que tuvieran que ver con seguridad y hackeo, algo que no se veía mal a simple vista, pues era una comunidad de personas a las que les gustaba el tema. Cabe anotar, que este sitio tenía toda la tecnología necesaria tanto en equipos, como en redes y software, además de un restaurante para no tener que desplazarse o salir. Todo se veía muy transparente a simple vista.

Algunos hackers al ver tanta generosidad y un proyecto tan grande, empezaron a preguntar y encontraron la siguiente respuesta: "…*un partido político de mala reputación y una organización que nada tenía que ir a buscar a un espacio como esos*…"[20].

Buggly no resulto ser otra cosa que una fachada para la operación Andrómeda creada por la Central de Inteligencia Técnica del Ejército Nacional y el sr. Bender resulto ser un cabo del ejercito que requería obtener conocimiento de informática, de hacking ético y que estaba reclutando los mejores hackers para sus operaciones sin que estos se dieran cuenta.

Ya aquí podemos empezar a analizar la situación ética del caso, ya que se va configurando la intensión de usar a las personas para fines políticos y mediante engaños obtener información sobre técnicas y conocimientos en ciertos campos de seguridad, además, del dinero de origen dudoso invertido que se utilizaba para

---

20 ENTER.CO. Detrás de Buggly: la historia de la fachada Andrómeda. [Consulta: 11 de septiembre del 2022]. [Página Web]. Disponible en:HTTPS://WWW.ENTER.CO/EMPRESAS/COLOMBIA-DIGITAL/DETRAS-DE-BUGGLY-LA-HISTORIA-DE-LA-FACHADA-ANDROMEDA/

poder generar espacios donde el conocimiento se pudiera compartir sin mayores cuestionamientos.

En el informe de la revista semana cita: "…*En la fachada de la Operación Andrómeda no se aplicó el principio del secreto, establecido por la inteligencia militar para este tipo de actividades. No se realizó un detallado estudio de seguridad del personal para la selección de los agentes que integraron la operación", reconoce la comisión en otro de los puntos. Si bien aclara que la fachada estaba amparada por la ley para realizar labores de inteligencia, acepta que debido a la falta de controles y al desorden algunos de sus integrantes se desviaron de su misión y terminaron relacionados a nivel individual en actividades ilegales*…"[21]

Podemos ver que la falta de controles al momento de revisar las hojas de vida, el historial de las personas que participaron en la operación, la falta de planeación pudo haber llevado a que extralimitara las actividades de alguno de los integrantes sin que hubiera quien las supervisara.

La investigación también indica que al hacker Andres Sepúlveda se le dio información confidencial, y esto lo justificaron indicando errores en el manejo de la de seguridad con el manejo de dicha información y de la documentación. Grave delito que es penalizado según la ley 1273 de 2009 articulo 269H en sus numerales del 2 al 7.

[21] Semana.com. El informe que sacudió el caso de la fachada Andrómeda. [Consulta: 11 de septiembre del 2022]. [Página Web]. Disponible en: https://www.semana.com/nacion/articulo/el-informe-que-sacudio-el-caso-de-la-fachada-andromeda/415642-3/

También hay indicios en varios informes que apuntan a que a que la prioridad era hacer espionaje a los computadores de los negociadores de las Farc y el ELN para obtener información de estas guerrillas; además, indican que Buggly tenía las herramientas y software de interceptación de uso excluso de los gobiernos o que obtenían del mercado negro.

Analizando la situación podemos deducir que no les importaba cometer delitos informáticos porque se sentían protegidos y confiados de que nadie se daría cuenta por la fachada que manejaban. Podemos ver en los párrafos anteriores que definitivamente incurrieron en delitos según la ley 1373 de 2009 en su artículo 269A. donde condena el ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.

Lo más grave del caso es que Andrómeda estaba dentro del marco legal con la creación de la fachada "*Buggly Hacker*", legalmente constituidos con fundamento en la Constitución Política de Colombia, con directivas, reglamentos y manuales, a simple vista todo estaba correcto y se cumplía con las normas y estándares establecidos para los fines de Buggly.

A pesar de aparentar tener todo bajo la normatividad correspondiente la fiscalía acuso y mando a detener a varios agentes, oficiales, tenientes, cabos por el delito de espionaje, violación de datos y venta de información confidencial a terceros violando así los siguientes artículos de la ley 1373 de 2009: "Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO, Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS, Artículo 269E. USO DE SOFTWARE MALICIOSO, Artículo 269F. VIOLACIÓN DE DATOS PERSONALES, Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES, Artículo 2691. HURTO POR MEDIOS INFORMÁTICOS Y

SEMEJANTES, Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS."[22]

Andrómeda fue una operación de inteligencia militar que a pesar de haber creado una fachada como "*Buggly Hacker*" esta se salió del control de los altos mandos y se prestó para que se presentaran actividades ilícitas dentro del proyecto, haciendo estallar el escándalo que se conoció.

4. ETAPA 3 - EJECUCIÓN PRUEBAS DE INTRUSIÓN

4.1 Descripción de herramientas utilizadas

La principal herramienta utilizada para realizar el laboratorio fue nmap y sus múltiples comandos.

Otra herramienta que se pretende utilizar es Nexus

4.2 Identificación de datos e información

Los datos más importantes y relevantes con los que se cuentan son:

- equipos de cómputo de los cuales se sospecha cuentan con Windows 7 X86 y X64.
- Equipos con S.O. antiguo.
- Una aplicación que sólo funciona en dicho S.O.

---

[22] DELITOS INFORMÁTICOS EN COLOMBIA. LEYES, PENAL. julio 26 de 2019. [Consulta: 09 de septiembre del 2022]. [En línea]. Disponible en: https://www.notaria19bogota.com/delitos-informaticos-en-colombia

- No se pueden reemplazar los S.O la aplicación no está migrada con compatibilidad a otros sistemas operativos.
- Los equipos de cómputo cuentan con un SMBv1 activo para compartir impresoras y algunos archivos dentro de la red.
- Hubo fuga de información (10 de junio de 2022) los S.O. no se encontraban actualizados, y su última actualización fue el 05 de febrero de 2017.
- La no actualización de los S.O. pudieron causar el fallo de seguridad con identificador CVE-2017-0144.
- Los equipos no tienen instalada la actualización MS17-010.

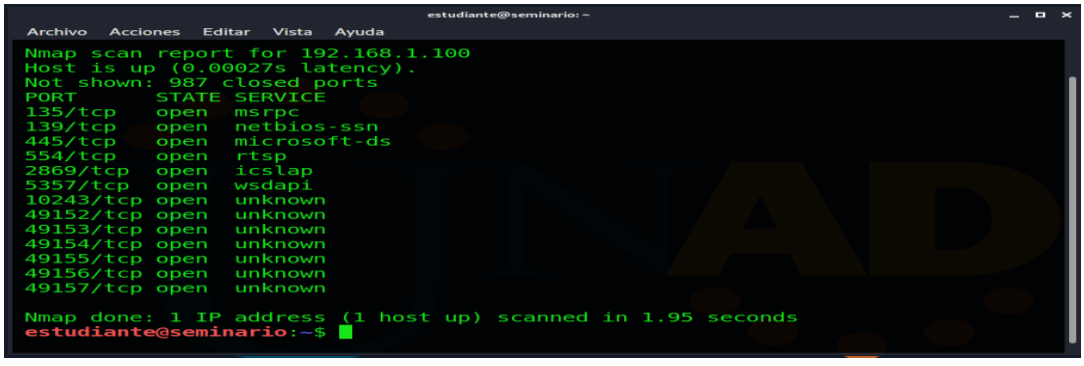
4.3 Herramientas utilizadas para identifcar los fallos

Herramientas utilizadas

NMAP: Con esta herramienta se comenzó

Inicialmente vamos a revisar los puestos abiertos dentro de la máquina.

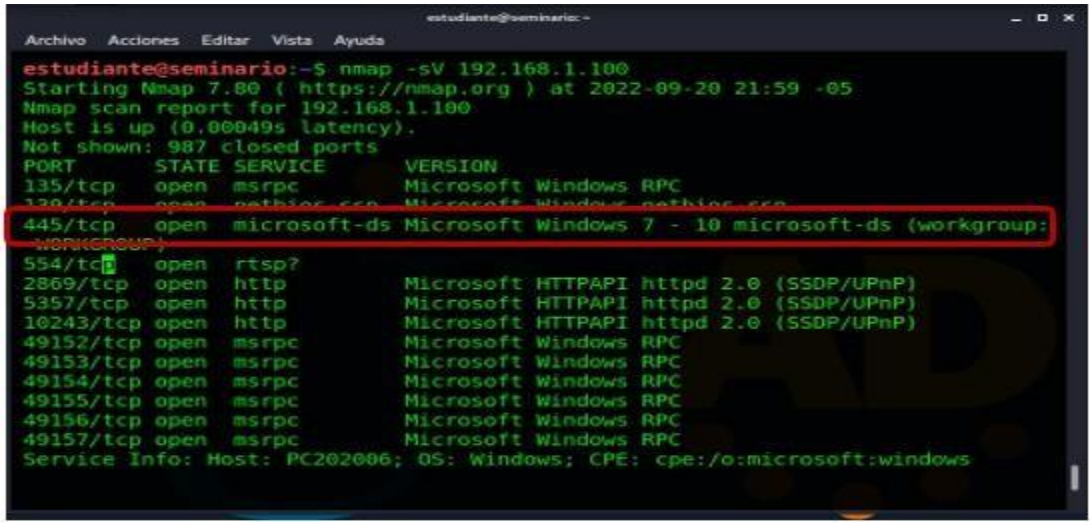
Ilustración 32. verificación de puertos abiertos en Windows 7 x64 – 192.168.1.100



Fuente: Propia

Luego, pasamos a ver más a fondo estos puertos y los servicios que corren en ellos, evidenciando que el puerto 445 se encentra abierto, además se encuentra corriendo el servicio

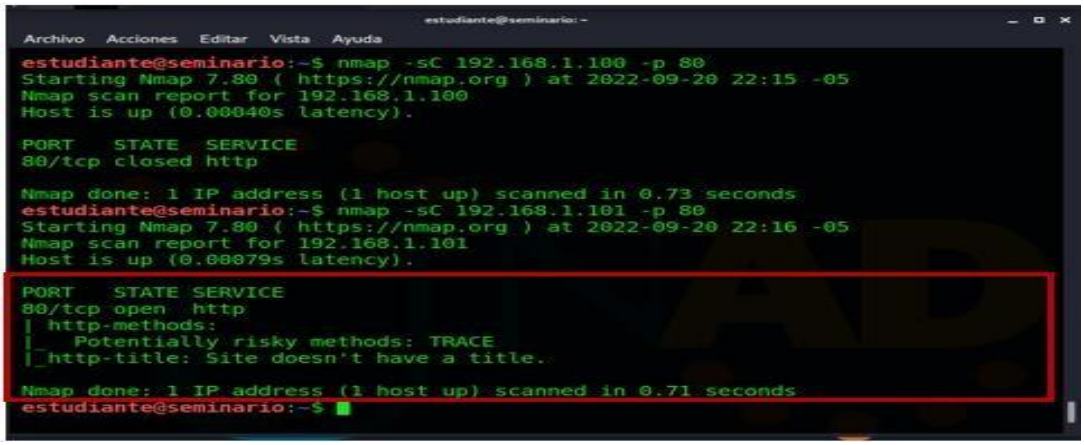
Ilustración 33. verificación de puertos abiertos y servicios comando nmap -sV



Fuente: Propia

También se Escaneo el puerto especifico 80 en la máquina de win 32 192.168.1.100 encontrando que es potencialmente peligroso.

Ilustración 34. Verificación puerto 80



Fuente: Propia

Ingresamos a la terminal Metasploit con el comando “msfconsole”, en modo administrador y usaremos el exploit eternalblue como se muestra a continuación:

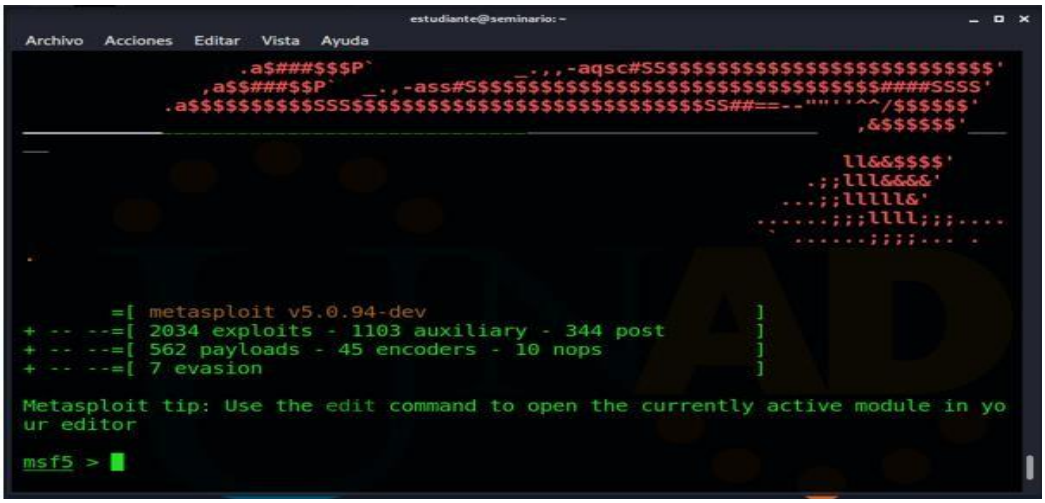
Ilustración 35. Ingresamos el comando msfconsole

Fuente: Propia

Ilustración 36. Corremos el comando msfconsole en Win 7 x64

Fuente: Propia

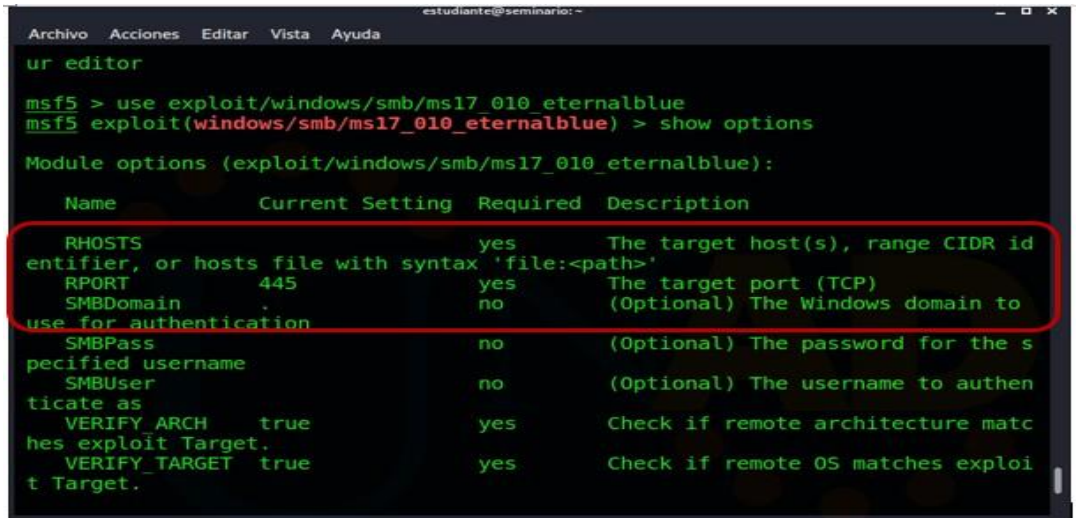
Ilustración 37. Visualización del comando metasploit



Fuente: Propia

Colocamos el comando ***show options*** para ver las opciones disponibles para el exploit.

Ilustración 38. Opciones RHOST y RPORT

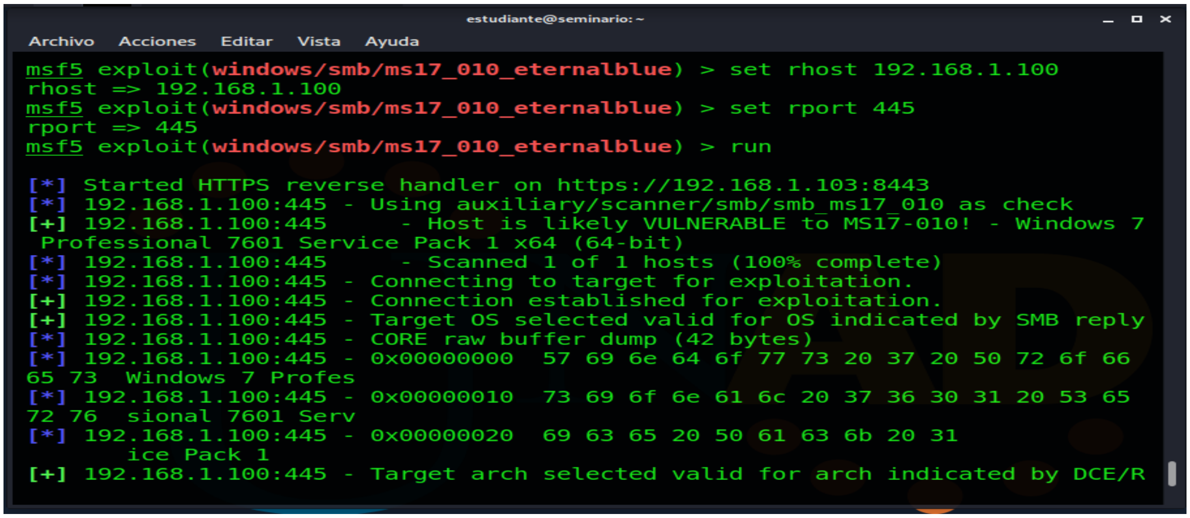


Fuente: Propia

Se realizará la prueba con las opciones arriba señaladas y se ejecuta el comando set RHOSSDT 192.168.1.100 – set RPORT 445 -Run. Qu se mencionan en la figura

7, sin embargo, lanzó una respuesta negativa.

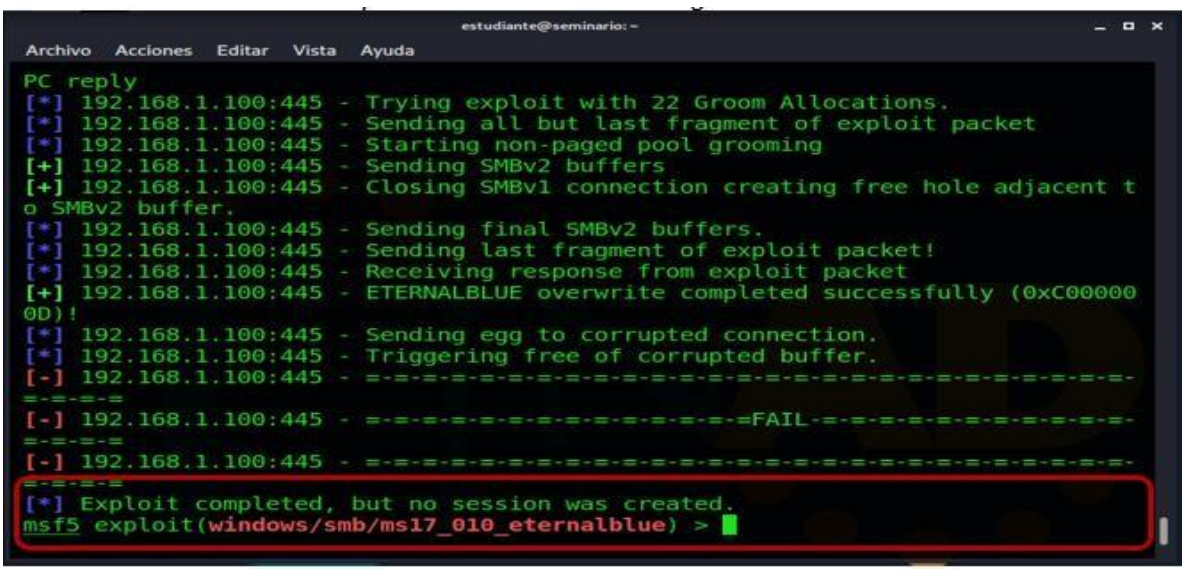
Ilustración 39. Se ejecutan Opciones RHOST y RPORT



Fuente: Propia

Al terminar la operación nos arroja error de acceso denegado.

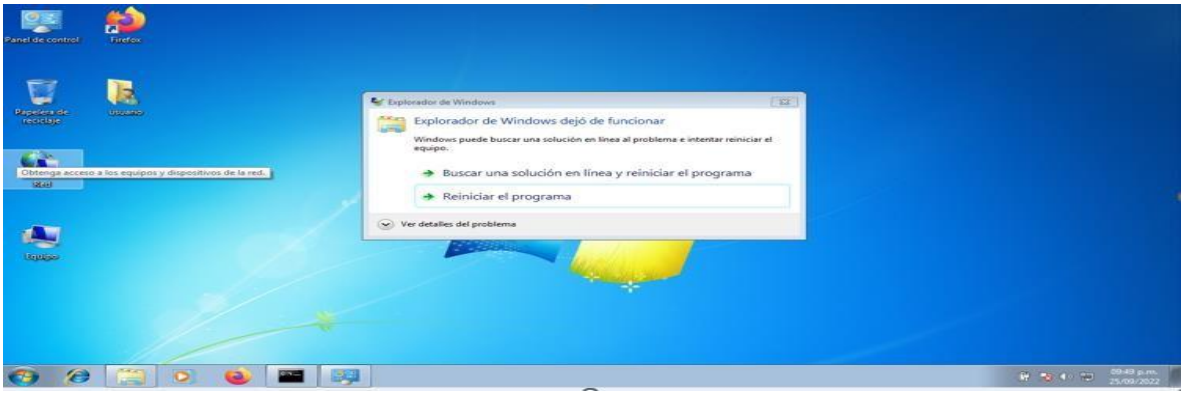
Ilustración 40. Proceso de la operación con resultado negativo



Fuente: Propia

Sin embargo, al ejecutarse el comando se pudo evidenciar que la máquina con el Win 7 x64 arrojo el siguiente error:

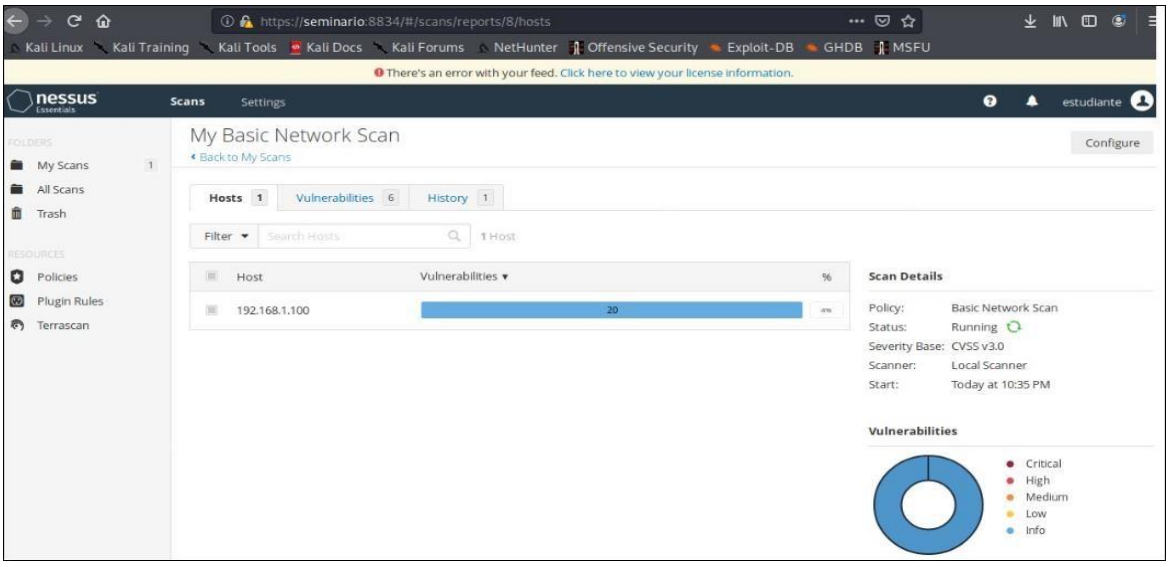
Ilustración 41. Ventana de error en Windows 7 x64



Fuente: Propia

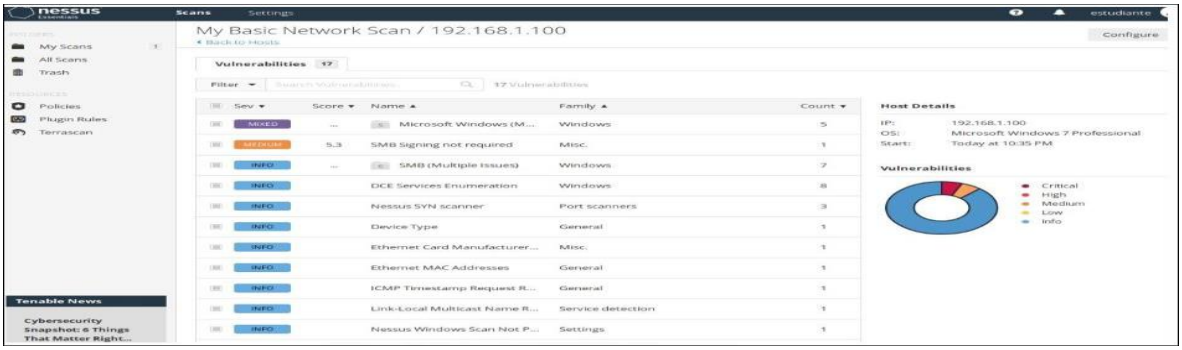
Por otro lado, se realizó el escaneo de vulnerabilidades con la herramienta NESSUX

Ilustración 42. Escaneo básico



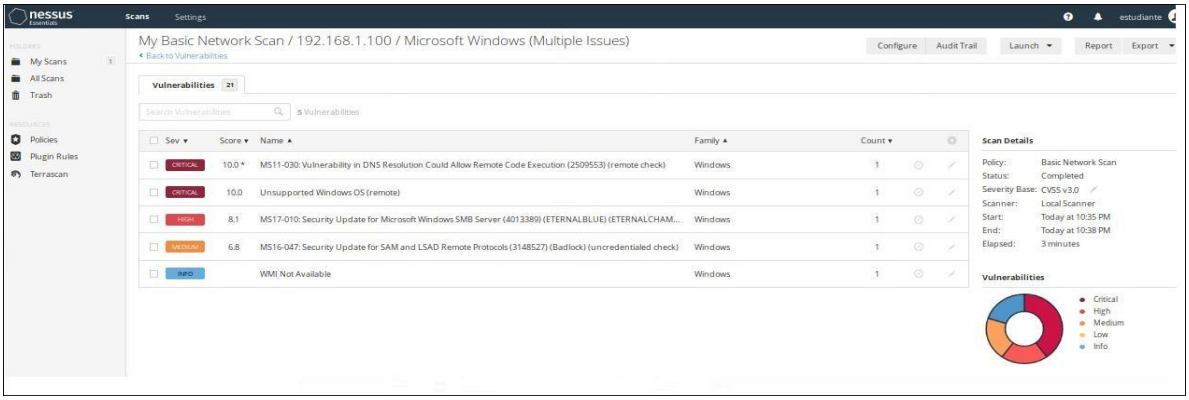
Fuente: Propia

Ilustración 43. Vulnerabilidades encontradas



Fuente: Propia

Ilustración 44. Vulnerabilidades criticas encontradas



Fuente: Propia

VULNERABILIDADES CRÍTICAS:

MS11-030: Vulnerabilidad en DNS La resolución podría permitir la ejecución remota de código (2509553 (comprobación remota)[22].

MS17-010: Actualización de seguridad para el servidor SMB de Microsoft Windows.

Existen múltiples vulnerabilidades de ejecución remota de código en Microsoft

server Message[23].

4.4 EXPLICACIÓN DEL ATAQUE

Inicialmente al tratar de ejecutar el exploit se notó que inmediatamente se la respuesta negativa, a pesar de realizar los pasos que se recomiendan, no hubo acceso a la máquina de Windows 7 x64 desde Kali, al ver que no había respuesta positiva, se decidió bajar el firewall y el Windows defender de la máquina de Windows 7 x64 para ver qué pasaba cuando el equipo carecía de protección, se volvieron a generar los pasos y el resultado mejoro, pero sin embargo se denegó el acceso con la diferencia de que se mostró el error en el explorador de Windows.

5. ETAPA 4 - CONTENCIÓN DE ATAQUES INFORMÁTICOS

5.1 Indagaciones preliminares frente a un ataque

En un ataque según lo solicitado en el anexo 5: "*Hackers Security solicita a sus integrantes de BlueTeam contener y sacar adelante un ataque informático el cual se está produciendo en tiempo real. La máquina que se debe analizar es la Windows 7 X64 analizada en la actividad anterior. La organización requiere un análisis exhaustivo de lo que está sucediendo a nivel técnico "sistema operativo, red", con la información recolectada se espera que dentro de su grado de experticia usted como miembro de un equipo Blue team logre contener el ataque para evitar que se genere más daño a nivel interno de la organización. Hackers Security le informa que*

[23] Microsoft. Actualización de seguridad para Windows Server de SMB: 14 de marzo de 2017. [Consulta: 09 de octubre del 2022]. [Página Web]. Disponible en: Microsoft. MS11-030: MS17-010: Actualización de seguridad para Windows Server de SMB: 14 de marzo de 2017. [Consulta: 09 de octubre del 2022]. [Página Web]. Disponible en: https://support.microsoft.com/es-es/topic/ms11-030-una-vulnerabilidad-en-la-resoluci%C3%B3n-dns-podr%C3%ADa-permitir-la-ejecuci%C3%B3n-remota-de-c%C3%B3digo-12-de-abril-2011-98cdc5e4-af92-597a-0a0b-49406f3c4134

no existe presupuesto para hacer uso de herramientas de pago, por ende, el experto en Ciberseguridad deberá optar por una serie de herramientas mínimo con licencia GPL."

Por lo general en ataques a redes lo que sucede es que el atacante escanea la red en busca de vulnerabilidades para propagarse lateralmente a otras partes de la red, por lo que lo primero que considero se debe hacer es aislar los sistemas afectados lo más rápido posible. Tan pronto como haya aislado los sistemas afectados, lo que seguiría es informar del ataque a las autoridades pertinentes, ya que esto puede ayudarlas a identificar a los posibles causantes que pueden seguir actuando en otras redes y así prepararlas para posibles ataques.

El siguiente paso sería identificar posible equipo inicial o "Paciente Cero" que puede ser la fuente de la infección. Lo que se pude hacer es identificar los cambios sucedidos y los usuarios que accedieron a esos archivos antes y durante el ataque. Identificando este usuario inicial lo que se debe hacer es deshabilitar su cuenta de inmediato para mitigar la posibilidad de una mayor infección y evitar que el ataque se siga propagando.

Cuando el ataque sucede por ransomware, lo primero que hacen las organizaciones es restaurar una copia de seguridad. Los atacantes son conscientes de esto y por eso, hacen todo lo posible para localizar las copias de seguridad y cifrarlas o eliminarlas. Las empresas siempre deben tratar de mantener una copia fuera de la red de sus copias de seguridad y asegurarse de que estén protegidas con contraseña u otro nivel de acceso.

Otra actividad que se debe hacer es detener temporalmente las tareas de mantenimiento que se realizan en la cotidianidad de la red y los sistemas. Lo anterior porque tareas como realizar actualizaciones o borrar temporales de los equipos,

puede alterar la investigación que se debe hacer para encontrar el origen y las vulnerabilidades de la red.

Un ejercicio que se puede realizar a continuación es realizar copia de seguridad de los sistemas infectados, lo que se puede hacer antes de formatear los equipos y reinstalar copias de seguridad o sistemas operativos desde cero. Lo anterior lo propongo, debido a que a veces se puede tratar de recuperar la información contenida en los sistemas o tener el respaldo en caso de una investigación.

Otro paso que se puede hacer es identificar el posible virus, ransomware o ataque, lo que permitirá determinar si existe ya desarrollado una solución a los daños que este allá dejado en los sistemas, así como la forma en que se puede propagar y los posibles puertos lo maneras de acceso a las redes de la entidad.

5.2. Medidas de hardenización

Después de conocer muy bien cada elemento o componente de los sistemas de información se propone:

- Crear ambientes de prueba con simulando la red de la empresa con la mayor precisión posible, probando las reglas y cambios antes de realizarlos en un ambiente real, esto con el fin de que al realizar los cambios de configuración los sistemas no se vayan a ver afectados.

- Luego, aplicar y dar cumplimiento a todas las reglas y cambios en la configuración de sistemas operativos o aplicativos en temas de seguridad generados en las máquinas en producción, verificando que todas las directivas están correctamente cargadas, como por ejemplo: que los puertos que no se usen se hallan cerrado correctamente, que los usuarios que no se requieran sean eliminados, que la configuración de las credenciales hayan

quedado robustas, que la configuración para que se bloquee la pantalla luego de cierto tiempo sea correcta y que la configuración para que solo admita protocolos robustos se cumpla, entre otros.

- Después realizar un monitoreo y supervisión constante, esperando con esto haber reforzado la seguridad de la infraestructura, porque, aunque no parezca es un proceso delicado, que, aunque tiene guía debe adecuarse al entono de cada empresa.

5.3 Diferencias entre blue team e incidentes

Un equipo Blue Team es el que defiende los ataques para los sistemas informáticos de una empresa realizando auditoras a DNS, efectuando análisis de red e infraestructura, instalando software de seguridad, entre otros, mientras que el "CSIRT" es un equipo de da respuestas a incidentes que se generan en los sistemas de información se dedica a implementar y gestionar medidas tecnológicas y su principal objetivo es mitigar el riesgo de ataques ocurridos contra los sistemas.

Los "CSIRT" pueden prestar mucha utilidad al momento de dar tratamiento a incidentes de servicios utilizando alertas y advertencias, análisis de incidentes, coordinando la respuesta a incidentes y las respuestas a incidentes en sitio de ser necesario, realizando análisis y tratamiento de vulnerabilidades. Hay servicios que pueden generar proactivamente como, por ejemplo: Comunicados, difusión de información relacionada con la seguridad, y auditorías de seguridad de los sistemas de información entre otros.

5.4 CIS “Center For Internet Security”

El Centro para la Seguridad de Internet (CIS) publica los Controles de Seguridad Críticos (CSC)[24] de CIS para ayudar a las organizaciones a defenderse mejor contra los ataques conocidos al generar los conceptos clave de seguridad en controles procesables y así lograr una mayor defensa de ciberseguridad general.

Si nos indican que debemos trabajar con CIS, entendería que debo seguir las recomendaciones actualizadas y concretas que emite esta entidad, que nos puede ayudar a mejorar nuestros lineamientos de seguridad a través de sus Controles de seguridad críticos para una ciberdefensa efectiva, lo que anteriormente conocidos como SANS.

El CIS-CSC, que actualmente está en la versión 7, fue creado por expertos de numerosas agencias gubernamentales y líderes de la industria y es universalmente aplicable a todas las organizaciones.
CIS separa los controles de seguridad en tres categorías: básicos, fundacionales y organizativos, independientemente del tipo de entidad. Esa priorización de estándares es lo que diferencia las recomendaciones del CIS CSC de otros controles y recomendaciones de seguridad.

EL CIS propone 20 controles críticos de seguridad, de los cuales los primeros seis en la lista se denominan controles "básicos" que deben implementar todas las organizaciones para la preparación de la defensa cibernética. Estos son: “

1) Inventario y Control de Activos de Hardware

[24] ciberseguridad. Métodos de búsqueda de amenazas de ciberseguridad. 28 de febrero de 2018. [Consulta: 09 de octubre del 2022]. [Página Web]. Disponible en: https://ciberseguridad.blog/metodos-de-busqueda-de-amenazas-de-ciberseguridad/

2) Inventario y Control de Activos de Software

3) Gestión continua de vulnerabilidades

4) Uso controlado de privilegios administrativos

5) Configuración segura de hardware y software en dispositivos móviles, portátiles, estaciones de trabajo y servidores

6) Mantenimiento, Monitoreo y Análisis de Registros de Auditoría"[25]

Para el equipo BlueTeam, seguir la guía de CIS para estos seis controles principales generará grandes beneficios para la empresa ya que es integral en su visión de lo que se requiere para una sólida defensa de ciberseguridad. Las recomendaciones de CIS abarcan no solo datos, software y hardware, sino también personas y procesos.

5.5 Funciones y características de un SIEM

SIEM (Security Information and Event Management): Es un sistema que permite analizar en tipo real logs y alertas para detectar y detener amenazas evitando que la infraestructura de la empresa sea atacada por ciberdelincuentes.

Principales características de un SEIM

- Funciona con referencias de orígenes diferentes: sistemas de seguridad.

[25] Universidad San Ignacio de Loyola. 2022. [Consulta: 09 de octubre del 2022]. [Documento PDF en Línea]. Disponible en: https://repositorio.usil.edu.pe/server/api/core/bitstreams/1f8197b4-f197-4d3a-bc66-df778ada7067/content

- Despliega variedad de reglas internas de reciprocidad, con lo cual se podrá determinar si hay alguna acción sospechosa.

- Sistema que es apta para crear alertas s cuando hay sospechas de posibles ataques cibernéticos o peligros dentro del sistema.

- Permite la visualización de los datos en cuadros de mando para obtener métricas y poder tomar las decisiones estratégicas necesarias en materia de seguridad informática.

- Puede almacenar información durante periodos de tiempo muy largo. Esto es una gran ventaja ya se puede revisar el proceso de una intrusión en la línea completa de tiempo: el antes, el durante y el después.

5.6 Herramientas de contención de ataques informáticos

Entre las herramientas de contención software encontramos:

- **Snort**: Es un software gratuito de detección de extraños que se basa en red y que utiliza código abierto más exactamente lenguaje de programación C. este cuenta con tres módulos:

- **Sniffer Mode:** Este realiza una traza de los paquetes que transitan por la red de la empresa. Se puede configurar para que se puedan ver distintos tipos de paquetes (TCP, UDP, ICMP).

- **Packet Logger Mode:** Aquí podemos crear reglas indicando que paquetes podemos guardar según los requerimientos de la empresa.

- **NIDS**. Esta herramienta otorga permisos para que se apliquen reglas más específicas a los paquetes que se trasmiten, las reglas se incluyen en el archivo de configuración que se pasa como parámetro al iniciar la herramienta del snort.

Heimdal Security: Es una solución EDR que realiza búsqueda de amenazas, bloqueo, monitoreo constantemente, escaneo en disco local y cloud, además cuando se agrega la opción para administrar los derechos de escritorio, cubre todas las recomendaciones de proyectos de seguridad de Gartner en una solución: Gestión de acceso privilegiado, Gestión de vulnerabilidad[26] y Detección y respuesta.

Winpatrol: Solución con funcionalidades y muy liviana que podemos encontrar.[27].

[26] GEETFLARE. 13 Herramientas EDR para detectar y responder a ataques cibernéticos rápidamente. . [Consulta: 09 de octubre del 2022]. [Página web]. Disponible en: https://geekflare.com/es/edr-tools/

[27] CRISTINA PÉREZ S, Detección De Intrusos Con Snort. 2015, http://docplayer.es/8675215-Deteccion-de-intrusos-consnort.html.

CONCLUSIONES

Se consulto y desgloso cada una de las leyes y decretos más relevantes que rigen en Colombia sobre delitos informáticos y protección de datos encontrando que desde 1980 aproximadamente el estado empezó a interesarse en el tema.

Se estudio sobre las diferentes pruebas de pentesting, encontrando que cada una cumple una función especial y única, que es una secuencia de actividades procedimentales para alcanzar el objetivo deseado sobre la seguridad de la empresa con los insumos dados por la misma.

Se definieron los términos y principales características de cada una de las herramientas análisis de seguridad que se vieron en el trabajo.

Se realizó el ejercicio del laboratorio 1 denominado “banco de trabajo” reconociendo, analizando y configurando las máquinas virtuales WIN7-2020, WIN7-2020-X64 Y KALI-SEMINARIO para dejarlas dentro de un entorno de red y luego hacer pruebas de verificación de conexión entre ellas.

Se revisó y desgloso cada una de las cláusulas del acuerdo de confidencialidad de HACKERS SECURITY, encontrando muchas irregularidades, mostrándolas en el trabajo argumentando el porqué de sus fragmentos ilegales.

Se mencionan los artículos violados dentro de los apartes del acuerdo que tienen fragmentos ilegales. Además de dar respuesta a la pregunta que se nos hace sobre la aplicación a un trabajo con acuerdos que tienen fragmentos ilegales.

Se estudia la noticia “Operación Andrómeda Buggly” y se hace un análisis mostrando las implicaciones de esta en el ámbito legal, jurídico e informático del país.

En este trabajo retomamos conceptos que deben estar presentes siempre como especialistas en seguridad informática, siempre realizando un análisis profundo de cada actividad que se realiza.

RECOMENDACIONES

Después de haber realizado el trabajo a profundidad se puede recomendar a las empresas busquen siempre asegurar la información, mejorar los canales de protección con las herramientas que realmente realicen una función de seguridad, que cumplan con estándares requeridos, que se adapten a las necesidades de cada entorno y sobre todo que cumplan con las leyes de cada nación.

En este trabajo se pueden observar algunas herramientas utilizadas, sin embargo, en el mundo de la ciberseguridad existen muchas que se adecuan a cada necesidad, al igual se pueden encontrar equipos preparados para afrontar cualquier situación desde cualquier frente ya se ofensivo o defensivo de acuerdo con las necesidades de las empresas

Se recomienda además tener siempre presente que la información debe salvaguardarse siempre, ya que es el mayor activo de las personas y de las empresas y cada vez más es más latente el peligro de un ataque para robarla o eliminarla.

BIBLIOGRAFÍA

DELITOS INFORMÁTICOS EN COLOMBIA. LEYES, PENAL. julio 26 de 2019. [Consulta: 30 de agosto del 2022]. [En línea]. Disponible en: https://www.notaria19bogota.com/delitos-informaticos-en-colombia

FASES DEL PENTESTING. 23 de febrero de 2017. [Consulta: 30 de agosto del 2022]. [En línea]. Disponible en: https://eastmadhack.benjagarrido.com/fases-del-pentesting/

Articulo por José Cuervo Álvarez. Legislación Informática de Colombia. [Consultado 30 de agosto de 2022]. [En Línea] http://www.informatica-juridica.com/legislacion/colombia/

PENTESTING PARA DUMMIES. MARTA VILA GÓMEZ. Abril 20 de 2022. [Consulta: 30 de agosto del 2022]. [En línea]. Disponible en: https://intelequia.com/blog/post/3231/pentesting-para-dummies

Protegeme. Herramientas de pentesting más utilizadas. [Consulta: 30 de agosto del 2022]. [En línea]. Disponible en: https://www.protegeme.es/herramientas-de-pentesting/

OPENWEBINARS. Qué es Metasploit framework. Héctor Rizaldos. Octubre 22 de 2018. [Consulta: 31 de agosto del 2022]. [Página Web]. Disponible en: https://openwebinars.net/blog/que-es-metasploit/

PcHardwarePro. ¿Qué es Metasploit y cómo utilizarlo correctamente? 2022. [Consulta: 31 de agosto del 2022]. [Página Web]. Disponible en:

https://www.pchardwarepro.com/que-es-metasploit-y-como-utilizarlo-correctamente/

NMAP.ORG. Guía de referencia de Nmap. 2022. [Consulta: 31 de agosto del 2022]. [BLOG]. Disponible en: https://nmap.org/man/es/index.html

Marin de la fuente. ¿Qué es Nmap? Por qué necesitas este mapeador de red. abril 29 de 2019. . [Consulta: 31 de agosto del 2022]. [Página Web]. Disponible en: https://www.marindelafuente.com.ar/

Informática Jurídica. Legislación Informática de Colombia. [Consulta: 31 de agosto del 2022]. [Página Web]. Disponible en: https://www.informatica-juridica.com/legislacion/colombia/

DELITOS INFORMÁTICOS EN COLOMBIA. LEYES, PENAL. julio 26 de 2019. [Consulta: 09 de septiembre del 2022]. [En línea]. Disponible en: https://www.notaria19bogota.com/delitos-informaticos-en-colombia

ENTER.CO. Detrás de Buggly: la historia de la fachada Andrómeda. [Consulta: 11 de septiembre del 2022]. [Página Web]. Disponible en: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

Semana.com. El informe que sacudió el caso de la fachada Andrómeda. [Consulta: 11 de septiembre del 2022]. [Página Web]. Disponible en:

https://www.semana.com/nacion/articulo/el-informe-que-sacudio-el-caso-de-la-fachada-andromeda/415642-3/

Tenable. Nessus. Vaya un paso adelante de los atacantes. 2022. [Consulta: 20 de septiembre del 2022]. [En línea]. Disponible en: https://es-la.tenable.com/lp/campaigns/20/try-nessus/?utm_campaign=gs-{16572891347}-{139751764532}-{587683863011}_00023809&utm_promoter=tenable-hv-brand-00023809&utm_source=google&utm_term=nessus&utm_medium=cpc&utm_geo=latam&gclid=CjwKCAjwm8WZBhBUEiwA178UnG7LaU7Rt447h9KQLXXQkDK9RJk TQxfdE77Z-cZWhG82Nz3kjX5mLhoCNXcQAvD_BwE

NMAP.ORG. Guía de referencia de Nmap. 2022. [Consulta: 20 de septiembre del 2022]. [BLOG]. Disponible en: https://nmap.org/man/es/index.html

MUNDOHACKERS. [Consulta: 20 de septiembre del 2022]. [BLOG]. Disponible en: https://mundo-hackers.weebly.com/masscan.html

CIS Critical Security Controls.How these controls apply to your organization. [Consulta 02 de octubre de 2022]. [En línea]. Disponible en: https://www.rapid7.com/fundamentals/cis-critical-security-controls/

LEPIDE. How to React to Ransomware Attack in 8 Steps. [Consulta 02 de octubre de 2022]. [En línea]. Disponible en: https://www.lepide.com/blog/how-to-react-to-ransomware-attack-in-8-steps/

GEEKFLARE. 13 herramientas gratuitas en línea para analizar las vulnerabilidades y el malware de seguridad de sitios web. 06 de septiembre de 2022. [Consulta 02

de octubre de 2022]. [En línea]. Disponible en: https://geekflare.com/es/online-scan-website-security-vulnerabilities/.

Osctec. Pentest: las 10 mejores herramientas usadas en el mercado. 2022. [Consulta: 09 de octubre del 2022]. [Página Web]. Disponible en: https://ostec.blog/es/aprendizaje-descubrimiento/pentest-las-10-mejores-herramientas-usadas-en-el-mercado/

Osctec. Pentest, todo lo que debe saber. 25 de mayo 2022. [Consulta: 09 de octubre del 2022]. [Página Web]. Disponible en: https://ostec.blog/es/seguridad/pentest-todo-lo-que-debe-saber/

Policia Nacional. Normatividad sobre delitos informáticos. 2022. [Consulta: 08 de octubre del 2022]. [Página Web]. Disponible en: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

COLOMBIA. CONGRESO DE LA REPBLICA. Ley 1273 de 2009.“de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. [En línea].Bogotá D.C., Diario Oficial. 2009. 47.223 Disponible https://www.enticconfio.gov.co/images/stories/normatividad/Ley_1273_de_2009%20.pdf

Microsoft. MS11-030: MS17-010: Actualización de seguridad para Windows Server de SMB: 14 de marzo de 2017. [Consulta: 09 de octubre del 2022]. [Página Web].

Disponible en: https://support.microsoft.com/es-es/topic/ms11-030-una-vulnerabilidad-en-la-resoluci%C3%B3n-dns-podr%C3%ADa-permitir-la-ejecuci%C3%B3n-remota-de-c%C3%B3digo-12-de-abril-2011-98cdc5e4-af92-597a-0a0b-49406f3c4134

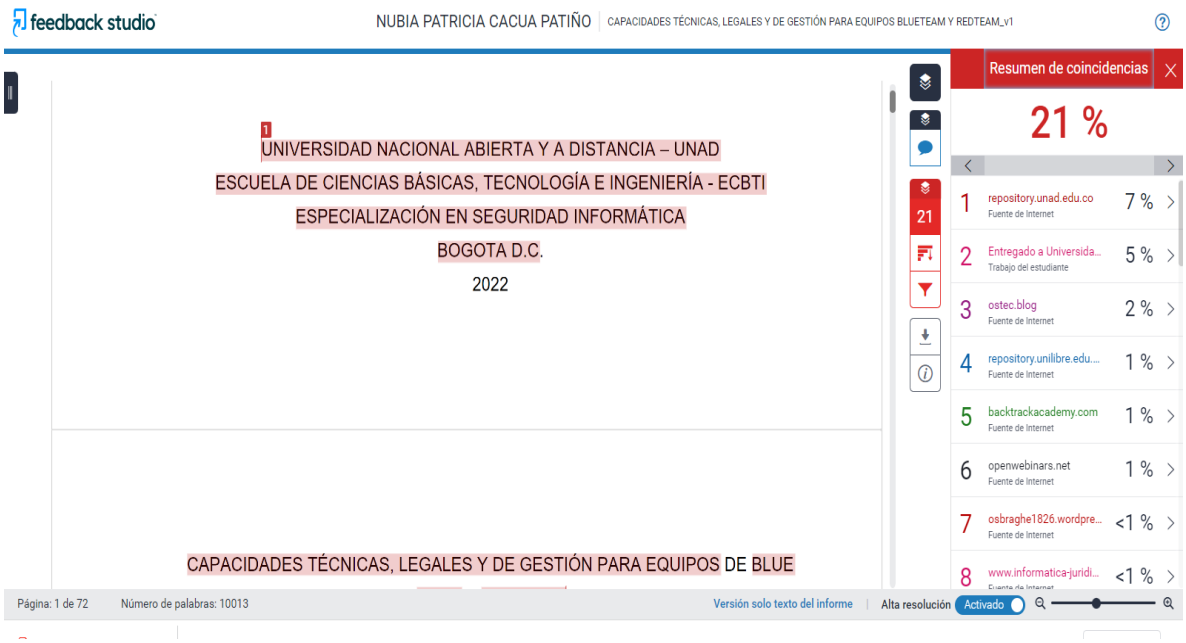
ciberseguridad. Métodos de búsqueda de amenazas de ciberseguridad. 28 de febrero de 2018. [Consulta: 09 de octubre del 2022]. [Página Web]. Disponible en: https://ciberseguridad.blog/metodos-de-busqueda-de-amenazas-de-ciberseguridad/

Microsoft. MS11-030: Una vulnerabilidad en la resolución DNS podría permitir la ejecución remota de código: 12 de abril de 2011. [Consulta: 09 de octubre del 2022]. [Página Web]. Disponible en: https://support.microsoft.com/es-es/topic/ms11-030-una-vulnerabilidad-en-la-resoluci%C3%B3n-dns-podr%C3%ADa-permitir-la-ejecuci%C3%B3n-remota-de-c%C3%B3digo-12-de-abril-2011-98cdc5e4-af92-597a-0a0b-49406f3c4134

Universidad San ignacio de Loyola. 2022. [Consulta: 09 de octubre del 2022]. [Documento PDF en Línea]. Disponible en: https://repositorio.usil.edu.pe/server/api/core/bitstreams/1f8197b4-f197-4d3a-bc66-df778ada7067/content

ANEXOS

ENTREGA DE RESULTADO TURNITING



Link del Video:

video_sustentacion.mp4